



# RUGGEDCOM ROS v4.2.2.F

User Guide

For RS900GPF

04/2018  
RC1230-EN-01

Preface	
Introduction	1
Using ROS	2
Getting Started	3
Device Management	4
System Administration	5
Security	6
Layer 2	7
Traffic Control and Classification	8
Time Services	9
Network Discovery and Management	10
IP Address Assignment	11
Troubleshooting	12

Copyright © 2018 Siemens Canada Ltd

All rights reserved. Dissemination or reproduction of this document, or evaluation and communication of its contents, is not authorized except where expressly permitted. Violations are liable for damages. All rights reserved, particularly for the purposes of patent application or trademark registration.

This document contains proprietary information, which is protected by copyright. All rights are reserved. No part of this document may be photocopied, reproduced or translated to another language without the prior written consent of Siemens Canada Ltd.

## » Disclaimer Of Liability

Siemens has verified the contents of this document against the hardware and/or software described. However, deviations between the product and the documentation may exist.

Siemens shall not be liable for any errors or omissions contained herein or for consequential damages in connection with the furnishing, performance, or use of this material.

The information given in this document is reviewed regularly and any necessary corrections will be included in subsequent editions. We appreciate any suggested improvements. We reserve the right to make technical improvements without notice.

## » Registered Trademarks

RUGGEDCOM™ and ROS™ are trademarks of Siemens Canada Ltd.

Other designations in this manual might be trademarks whose use by third parties for their own purposes would infringe the rights of the owner.

## » Third Party Copyrights

Siemens recognizes the following third party copyrights:

- Copyright © 2004 GoAhead Software, Inc. All Rights Reserved.

## » Open Source

RUGGEDCOM ROS-F contains Open Source Software. For license conditions, refer to the associated *License Conditions* document.

## » Security Information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, machines, equipment and/or networks. They are important components in a holistic industrial security concept. With this in mind, Siemens' products and solutions undergo continuous development. Siemens recommends strongly that you regularly check for product updates.

For the secure operation of Siemens products and solutions, it is necessary to take suitable preventive action (e.g. cell protection concept) and integrate each component into a holistic, state-of-the-art industrial security concept. Third-party products that may be in use should also be considered. For more information about industrial security, visit <https://www.siemens.com/industrialsecurity>.

To stay informed about product updates as they occur, sign up for a product-specific newsletter. For more information, visit <https://support.automation.siemens.com>.

## » Warranty

Refer to the License Agreement for the applicable warranty terms and conditions, if any.

For warranty details, visit <https://www.siemens.com/ruggedcom> or contact a Siemens customer service representative.

## » Contacting Siemens

### **Address**

Siemens Canada Ltd  
Industry Sector  
300 Applewood Crescent  
Concord, Ontario  
Canada, L4K 5C7

### **Telephone**

Toll-free: 1 888 264 0006  
Tel: +1 905 856 5288  
Fax: +1 905 856 1995

### **E-mail**

[ruggedcom.info.i-ia@siemens.com](mailto:ruggedcom.info.i-ia@siemens.com)

### **Web**

<https://www.siemens.com/ruggedcom>



# Table of Contents

Preface .....	xiii
Conventions .....	xiii
Related Documents .....	xiv
System Requirements .....	xv
Accessing Documentation .....	xv
Training .....	xv
Customer Support .....	xvi
Chapter 1	
Introduction .....	1
1.1 Features and Benefits .....	1
1.2 Security Recommendations .....	3
1.3 Supported Networking Standards .....	5
1.4 Port Numbering Scheme .....	6
1.5 Available Services by Port .....	6
1.6 FIPS Self-Tests .....	8
1.6.1 FIPS Power Up Self-Tests .....	8
1.6.2 FIPS Runtime Tests .....	9
1.6.3 Manually Launching FIPS Cryptographic Algorithm Tests .....	9
Chapter 2	
Using ROS .....	11
2.1 Logging In .....	11
2.2 Logging Out .....	12
2.3 Using the Web Interface .....	13
2.4 Using the Console Interface .....	14
2.5 Using the Command Line Interface .....	16
2.5.1 Available CLI Commands .....	16
2.5.2 Tracing Events .....	20
2.5.3 Executing Commands Remotely via RSH .....	21
2.5.4 Executing Secure Commands Remotely via SSH .....	21
2.5.5 Using SQL Commands .....	22
2.5.5.1 Finding the Correct Table .....	22
2.5.5.2 Retrieving Information .....	23
2.5.5.3 Changing Values in a Table .....	24

2.5.5.4	Resetting a Table .....	25
2.5.5.5	Using RSH and SQL .....	25
2.6	Selecting Ports in RUGGEDCOM ROS .....	25
2.7	Managing the Flash File System .....	26
2.7.1	Viewing a List of Flash Files .....	26
2.7.2	Viewing Flash File Details .....	27
2.7.3	Defragmenting the Flash File System .....	27
2.8	Accessing Maintenance Mode .....	27
Chapter 3		
<b>Getting Started .....</b>		<b>29</b>
3.1	Connecting to ROS .....	29
3.1.1	Default IP Address .....	29
3.1.2	Connecting Directly .....	29
3.1.3	Connecting Remotely .....	30
3.2	Configuring a Basic Network .....	31
Chapter 4		
<b>Device Management .....</b>		<b>33</b>
4.1	Viewing Product Information .....	33
4.2	Viewing CPU Diagnostics .....	35
4.3	Restoring Factory Defaults .....	36
4.4	Uploading/Downloading Files .....	37
4.4.1	Uploading/Downloading Files Using XMODEM .....	38
4.4.2	Uploading/Downloading Files Using a TFTP Client .....	39
4.4.3	Uploading/Downloading Files Using a TFTP Server .....	39
4.4.4	Uploading/Downloading Files Using an SFTP Server .....	40
4.5	Managing Logs .....	41
4.5.1	Viewing Local and System Logs .....	41
4.5.2	Clearing Local and System Logs .....	41
4.5.3	Configuring the Local System Log .....	42
4.5.4	Managing Remote Logging .....	43
4.5.4.1	Configuring the Remote Syslog Client .....	43
4.5.4.2	Viewing a List of Remote Syslog Servers .....	44
4.5.4.3	Adding a Remote Syslog Server .....	44
4.5.4.4	Deleting a Remote Syslog Server .....	46
4.5.5	Transferring Secure Audit Logs .....	47
4.6	Managing Ethernet Ports .....	47
4.6.1	Controller Protection Through Link Fault Indication (LFI) .....	48
4.6.2	Viewing the Status of Ethernet Ports .....	49
4.6.3	Viewing Statistics for All Ethernet Ports .....	50

4.6.4	Viewing Statistics for Specific Ethernet Ports .....	50
4.6.5	Clearing Statistics for Specific Ethernet Ports .....	53
4.6.6	Configuring an Ethernet Port .....	53
4.6.7	Configuring Port Rate Limiting .....	56
4.6.8	Configuring Port Mirroring .....	58
4.6.9	Configuring Link Detection .....	59
4.6.10	Managing SFP Transceivers .....	60
4.6.10.1	SFP Transceiver Requirements .....	61
4.6.10.2	Monitoring an SFP Port .....	61
4.6.10.3	Displaying Information for an SFP Port .....	62
4.6.11	Managing PoE Ports .....	63
4.6.11.1	Configuring PoE Ports Globally .....	63
4.6.11.2	Configuring a Specific PoE Port .....	64
4.6.11.3	Scheduling PoE Ports .....	66
4.6.12	Detecting Cable Faults .....	68
4.6.12.1	Viewing Cable Diagnostics Results .....	68
4.6.12.2	Performing Cable Diagnostics .....	70
4.6.12.3	Clearing Cable Diagnostics .....	72
4.6.12.4	Determining the Estimated Distance To Fault (DTF) .....	72
4.6.13	Resetting Ethernet Ports .....	73
4.7	Managing IP Interfaces .....	73
4.7.1	Viewing a List of IP Interfaces .....	74
4.7.2	Adding an IP Interface .....	74
4.7.3	Deleting an IP Interface .....	76
4.8	Managing IP Gateways .....	77
4.8.1	Viewing a List of IP Gateways .....	77
4.8.2	Adding an IP Gateway .....	78
4.8.3	Deleting an IP Gateway .....	79
4.9	Configuring DNS Servers .....	80
4.10	Configuring IP Services .....	81
4.11	Managing Remote Monitoring .....	83
4.11.1	Managing RMON History Controls .....	84
4.11.1.1	Viewing a List of RMON History Controls .....	84
4.11.1.2	Adding an RMON History Control .....	84
4.11.1.3	Deleting an RMON History Control .....	86
4.11.2	Managing RMON Alarms .....	87
4.11.2.1	Viewing a List of RMON Alarms .....	88
4.11.2.2	Adding an RMON Alarm .....	89
4.11.2.3	Deleting an RMON Alarm .....	91
4.11.3	Managing RMON Events .....	92

4.11.3.1	Viewing a List of RMON Events .....	93
4.11.3.2	Adding an RMON Event .....	93
4.11.3.3	Deleting an RMON Event .....	95
4.12	Upgrading/Downgrading Firmware .....	95
4.12.1	Upgrading Firmware .....	96
4.12.2	Downgrading Firmware .....	96
4.13	Resetting the Device .....	97
4.14	Clearing Data .....	98
Chapter 5		
	<b>System Administration .....</b>	<b>99</b>
5.1	Configuring the System Information .....	99
5.2	Customizing the Login Screen .....	100
5.3	Enabling/Disabling the Web Interface .....	100
5.4	Managing Alarms .....	101
5.4.1	Viewing a List of Pre-Configured Alarms .....	101
5.4.2	Viewing and Clearing Latched Alarms .....	102
5.4.3	Configuring an Alarm .....	103
5.4.4	Authentication Related Security Alarms .....	106
5.4.4.1	Security Alarms for Login Authentication .....	106
5.4.4.2	Security Messages for Port Authentication .....	108
5.5	Managing the Configuration File .....	109
5.5.1	Updating the Configuration File .....	109
Chapter 6		
	<b>Security .....</b>	<b>111</b>
6.1	Managing Passwords .....	111
6.1.1	Configuring Passwords .....	112
6.1.2	Resetting Passwords .....	114
6.2	Clearing Private Data .....	115
6.3	Managing User Authentication .....	115
6.3.1	Managing RADIUS Authentication .....	115
6.3.1.1	Configuring RADIUS Authentication .....	116
6.3.1.2	Configuring the RADIUS Server .....	117
6.3.1.3	Configuring the RADIUS Client on the Device .....	117
6.3.2	Managing TACACS+ Authentication .....	119
6.3.2.1	Configuring TACACS+ .....	119
6.3.2.2	Configuring User Privileges .....	120
6.4	Managing Port Security .....	121
6.4.1	Port Security Concepts .....	122
6.4.1.1	Static MAC Address-Based Authentication .....	122



6.4.1.2	IEEE 802.1x Authentication .....	122
6.4.1.3	IEEE 802.1X Authentication with MAC Address-Based Authentication .....	123
6.4.1.4	Assigning VLANS with Tunnel Attributes .....	124
6.4.2	Viewing a List of Authorized MAC Addresses .....	124
6.4.3	Configuring Port Security .....	125
6.4.4	Configuring IEEE 802.1X .....	127
6.5	Managing SSH and SSL Keys and Certificates .....	129
6.5.1	SSL Certificates .....	130
6.5.2	SSH Host Key .....	131
6.5.3	Managing SSH Public Keys .....	131
6.5.3.1	Public Key Requirements .....	131
6.5.3.2	Adding a Public Key .....	132
6.5.3.3	Viewing a List of Public Keys .....	133
6.5.3.4	Updating a Public Key .....	133
6.5.3.5	Deleting a Public Key .....	134
6.5.4	Generating a Certificate Signing Request (CSR) .....	134
6.5.5	Certificate and Key Examples .....	136
Chapter 7		
Layer 2	.....	137
7.1	Managing Virtual LANs .....	137
7.1.1	VLAN Concepts .....	138
7.1.1.1	Tagged vs. Untagged Frames .....	138
7.1.1.2	Native VLAN .....	138
7.1.1.3	The Management VLAN .....	138
7.1.1.4	Edge and Trunk Port Types .....	139
7.1.1.5	Ingress and Egress Rules .....	139
7.1.1.6	Forbidden Ports List .....	140
7.1.1.7	VLAN-Aware and VLAN-Unaware Modes .....	140
7.1.1.8	GARP VLAN Registration Protocol (GVRP) .....	140
7.1.1.9	PVLAN Edge .....	142
7.1.1.10	QinQ .....	142
7.1.1.11	VLAN Advantages .....	143
7.1.2	Viewing a List of VLANs .....	145
7.1.3	Configuring VLANs Globally .....	145
7.1.4	Configuring VLANs for Specific Ethernet Ports .....	146
7.1.5	Managing Static VLANs .....	148
7.1.5.1	Viewing a List of Static VLANs .....	149
7.1.5.2	Adding a Static VLAN .....	149
7.1.5.3	Deleting a Static VLAN .....	151
7.2	Managing MAC Addresses .....	152

7.2.1	Viewing a List of MAC Addresses .....	152
7.2.2	Configuring MAC Address Learning Options .....	153
7.2.3	Configuring MAC Address Flooding Options .....	154
7.2.4	Managing Static MAC Addresses .....	156
7.2.4.1	Viewing a List of Static MAC Addresses .....	156
7.2.4.2	Adding a Static MAC Address .....	156
7.2.4.3	Deleting a Static MAC Address .....	158
7.2.5	Purging All Dynamic MAC Addresses .....	159
7.3	Managing Multicast Filtering .....	160
7.3.1	Managing IGMP .....	160
7.3.1.1	IGMP Concepts .....	160
7.3.1.2	Viewing a List of Multicast Group Memberships .....	164
7.3.1.3	Viewing Forwarding Information for Multicast Groups .....	165
7.3.1.4	Configuring IGMP .....	165
7.3.2	Managing GMRP .....	167
7.3.2.1	GMRP Concepts .....	167
7.3.2.2	Viewing a Summary of Multicast Groups .....	170
7.3.2.3	Configuring GMRP Globally .....	170
7.3.2.4	Configuring GMRP for Specific Ethernet Ports .....	171
7.3.2.5	Viewing a List of Static Multicast Groups .....	173
7.3.2.6	Adding a Static Multicast Group .....	173
7.3.2.7	Deleting a Static Multicast Group .....	174
Chapter 8		
	<b>Traffic Control and Classification .....</b>	<b>177</b>
8.1	Managing Classes of Service .....	177
8.1.1	Configuring Classes of Service Globally .....	178
8.1.2	Configuring Classes of Service for Specific Ethernet Ports .....	179
8.1.3	Configuring Priority to CoS Mapping .....	180
8.1.4	Configuring DSCP to CoS Mapping .....	181
Chapter 9		
	<b>Time Services .....</b>	<b>183</b>
9.1	Configuring the Time and Date .....	183
9.2	Managing NTP .....	184
9.2.1	Enabling/Disabling NTP Service .....	184
9.2.2	Configuring NTP Servers .....	185
Chapter 10		
	<b>Network Discovery and Management .....</b>	<b>187</b>
10.1	Managing LLDP .....	187

10.1.1	Configuring LLDP Globally .....	188
10.1.2	Configuring LLDP for an Ethernet Port .....	189
10.1.3	Viewing Global Statistics and Advertised System Information .....	190
10.1.4	Viewing Statistics for LLDP Neighbors .....	191
10.1.5	Viewing Statistics for LLDP Ports .....	192
10.2	Managing SNMP .....	193
10.2.1	SNMP Management Interface Base (MIB) Support .....	194
10.2.1.1	Supported Standard MIBs .....	195
10.2.1.2	Supported Proprietary RUGGEDCOM MIBs .....	195
10.2.1.3	Supported Agent Capabilities .....	196
10.2.2	SNMP Traps .....	197
10.2.3	Managing SNMP Users .....	199
10.2.3.1	Viewing a List of SNMP Users .....	199
10.2.3.2	Adding an SNMP User .....	199
10.2.3.3	Deleting an SNMP User .....	202
10.2.4	Managing Security-to-Group Mapping .....	203
10.2.4.1	Viewing a List of Security-to-Group Maps .....	203
10.2.4.2	Adding a Security-to-Group Map .....	204
10.2.4.3	Deleting a Security-to-Group Map .....	205
10.2.5	Managing SNMP Groups .....	206
10.2.5.1	Viewing a List of SNMP Groups .....	207
10.2.5.2	Adding an SNMP Group .....	207
10.2.5.3	Deleting an SNMP Group .....	209
10.3	ModBus Management Support .....	209
10.3.1	ModBus Function Codes .....	210
10.3.2	ModBus Memory Map .....	211
10.3.3	Modbus Memory Formats .....	215
10.3.3.1	Text .....	216
10.3.3.2	Cmd .....	216
10.3.3.3	Uint16 .....	216
10.3.3.4	Uint32 .....	216
10.3.3.5	PortCmd .....	217
10.3.3.6	Alarm .....	217
10.3.3.7	PSStatusCmd .....	218
10.3.3.8	TruthValues .....	218
Chapter 11	IP Address Assignment .....	221
11.1	Configuring the DHCP Relay Agent .....	221

Chapter 12

<b>Troubleshooting</b> .....	223
12.1 General .....	223
12.2 Ethernet Ports .....	224
12.3 Spanning Tree .....	224
12.4 VLANs .....	226

# Preface

This guide describes v4.2.2.F of ROS (Rugged Operating System) running on the RUGGEDCOM RS900GPF. It contains instructions and guidelines on how to use the software, as well as some general theory.

It is intended for use by network technical support personnel who are familiar with the operation of networks. It is also recommended for use by network and system planners, system programmers, and line technicians.



## IMPORTANT!

*Some of the parameters and options described may not be available depending on variations in the device hardware. While every attempt is made to accurately describe the specific parameters and options available, this Guide should be used as a companion to the Help text included in the software.*

## CONTENTS

- [“Conventions”](#)
- [“Related Documents”](#)
- [“System Requirements”](#)
- [“Accessing Documentation”](#)
- [“Training”](#)
- [“Customer Support”](#)

# Conventions

This User Guide uses the following conventions to present information clearly and effectively.

## » Alerts

The following types of alerts are used when necessary to highlight important information.



## DANGER!

*DANGER alerts describe imminently hazardous situations that, if not avoided, will result in death or serious injury.*



## WARNING!

*WARNING alerts describe hazardous situations that, if not avoided, may result in serious injury and/or equipment damage.*



## CAUTION!

*CAUTION alerts describe hazardous situations that, if not avoided, may result in equipment damage.*

**IMPORTANT!**

*IMPORTANT alerts provide important information that should be known before performing a procedure or step, or using a feature.*

**NOTE**

*NOTE alerts provide additional information, such as facts, tips and details.*

## » CLI Command Syntax

The syntax of commands used in a Command Line Interface (CLI) is described according to the following conventions:

Example	Description
<b>command</b>	Commands are in bold.
<b>command</b> parameter	Parameters are in plain text.
<b>command</b> parameter1 parameter2	Parameters are listed in the order they must be entered.
<b>command</b> parameter1 <i>parameter2</i>	Parameters in italics must be replaced with a user-defined value.
<b>command</b> [ parameter1   parameter2 ]	Alternative parameters are separated by a vertical bar ( ). Square brackets indicate a required choice between two or more parameters.
<b>command</b> { parameter3   parameter4 }	Curly brackets indicate an optional parameter(s).
<b>command</b> parameter1 parameter2 { parameter3   parameter4 }	All commands and parameters are presented in the order they must be entered.

# Related Documents

## » Product Notes

Document Title	Link
RUGGEDCOM ROS Release Notes v4.2.2.F	<a href="https://support.industry.siemens.com/cs/ww/en/view/109757252">https://support.industry.siemens.com/cs/ww/en/view/109757252</a>

## » User/Reference Guides

Document Title	Link
RUGGEDCOM NMS v2.1 User Guide for Windows	<a href="https://support.industry.siemens.com/cs/ww/en/view/109737564">https://support.industry.siemens.com/cs/ww/en/view/109737564</a>
RUGGEDCOM NMS v2.1 User Guide for Linux	<a href="https://support.industry.siemens.com/cs/ww/en/view/109737563">https://support.industry.siemens.com/cs/ww/en/view/109737563</a>
RUGGEDCOM DIRECTOR v1.4 User Guide	<a href="https://support.industry.siemens.com/cs/ww/en/view/97691648">https://support.industry.siemens.com/cs/ww/en/view/97691648</a>
RUGGEDCOM EXPLORER v1.5 User Guide	<a href="https://support.industry.siemens.com/cs/ww/en/view/109480804">https://support.industry.siemens.com/cs/ww/en/view/109480804</a>
RUGGEDCOM PING v1.2 User Guide	<a href="https://support.industry.siemens.com/cs/ww/en/view/97674073">https://support.industry.siemens.com/cs/ww/en/view/97674073</a>

**» FAQs**

Document Title	Link
How Do You Configure the SMP Function in a RUGGEDCOM Switch with RUGGEDCOM ROS?	<a href="https://support.industry.siemens.com/cs/ww/en/view/109474615">https://support.industry.siemens.com/cs/ww/en/view/109474615</a>
How to Secure RUGGEDCOM ROS Devices Before and After Field Deployment?	<a href="https://support.industry.siemens.com/cs/ww/en/view/99858806">https://support.industry.siemens.com/cs/ww/en/view/99858806</a>
How to Implement Robust Ring Networks Using RSTP and eRSTP?	<a href="https://support.industry.siemens.com/cs/ww/en/view/109738240">https://support.industry.siemens.com/cs/ww/en/view/109738240</a>

**» Installation Guides**

Document Title	Link
RUGGEDCOM RS900GPF Installation Guide	<a href="https://support.industry.siemens.com/cs/ww/en/view/109757162">https://support.industry.siemens.com/cs/ww/en/view/109757162</a>

## System Requirements

Each workstation used to connect to the RUGGEDCOM ROS interface must meet the following system requirements:

- Must have one of the following Web browsers installed:
  - Microsoft Internet Explorer 8.0 or higher
  - Mozilla Firefox
  - Google Chrome
  - Iceweasel/IceCat (Linux Only)
- Must have a working Ethernet interface compatible with at least one of the port types on the RUGGEDCOM device
- The ability to configure an IP address and netmask on the computer's Ethernet interface

## Accessing Documentation

The latest user documentation for RUGGEDCOM ROS v4.2.2.F is available online at <https://www.siemens.com/ruggedcom>. To request or inquire about a user document, contact Siemens Customer Support.

## Training

Siemens offers a wide range of educational services ranging from in-house training of standard courses on networking, Ethernet switches and routers, to on-site customized courses tailored to the customer's needs, experience and application.

Siemens' Educational Services team thrives on providing our customers with the essential practical skills to make sure users have the right knowledge and expertise to understand the various technologies associated with critical communications network infrastructure technologies.

Siemens' unique mix of IT/Telecommunications expertise combined with domain knowledge in the utility, transportation and industrial markets, allows Siemens to provide training specific to the customer's application.

For more information about training services and course availability, visit <https://www.siemens.com/ruggedcom> or contact a Siemens Sales representative.

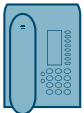
## Customer Support

Customer support is available 24 hours, 7 days a week for all Siemens customers. For technical support or general information, contact Siemens Customer Support through any of the following methods:



### Online

Visit <http://www.siemens.com/automation/support-request> to submit a Support Request (SR) or check on the status of an existing SR.



### Telephone

Call a local hotline center to submit a Support Request (SR). To locate a local hotline center, visit <http://www.automation.siemens.com/mcms/aspa-db/en/automation-technology/Pages/default.aspx>.



### Mobile App

Install the Industry Online Support app by Siemens AG on any Android, Apple iOS or Windows mobile device and be able to:

- Access Siemens' extensive library of support documentation, including FAQs and manuals
- Submit SRs or check on the status of an existing SR
- Contact a local Siemens representative from Sales, Technical Support, Training, etc.
- Ask questions or share knowledge with fellow Siemens customers and the support community



# 1 Introduction

Welcome to the RUGGEDCOM ROS v4.2.2.F Software User Guide for the RUGGEDCOM RS900GPF devices. This Guide describes the wide array of carrier grade features made available by RUGGEDCOM ROS (Rugged Operating System).

This chapter provides a basic overview of the RUGGEDCOM ROS software.

## CONTENTS

- [Section 1.1, “Features and Benefits”](#)
- [Section 1.2, “Security Recommendations”](#)
- [Section 1.3, “Supported Networking Standards”](#)
- [Section 1.4, “Port Numbering Scheme”](#)
- [Section 1.5, “Available Services by Port”](#)
- [Section 1.6, “FIPS Self-Tests”](#)

### Section 1.1

## Features and Benefits

The following describes the many features available in RUGGEDCOM ROS and their benefits:

- **FIPS Compliance**

FIPS 140-2 is a security standard produced by the U.S. National Institute of Standards and Technology (NIST) that outlines general requirements for cryptographic modules within computer and telecommunication systems.

RUGGEDCOM ROS has been developed to comply with the security requirements for this standard. For full compliance, the product must be configured according to the indications as described in the *FIPS 140-2 Non-Proprietary Security Policy*.

Running in FIPS mode (i.e. configured according to the guidelines in the *FIPS 140-2 Non-Proprietary Security Policy*) provides assurance that only FIPS approved ciphers are used, preventing weaker crypto or hash to be used.

RUGGEDCOM ROS supports a number of tests and procedures, run at startup and regularly during operation, to ensure the cryptographic module performs properly. It can detect errors in the operation of the cryptographic module and prevent the compromise of sensitive data and critical security parameters that could result from such errors.

For more information about the FIPS 140-2 Cryptographic Module Validation Program and a list of certified products, refer to <http://csrc.nist.gov/groups/STM/cmvp/index.html>.



### IMPORTANT!

*The following insecure protocols are disabled by default in RUGGEDCOM ROS: RADIUS, TACACS+, RSH, Telnet, TFTP, ModBus management, Remote Syslog, SNMPv1, SNMPv2 and SNMPv3. To meet*

*varied customer needs, these protocols can be enabled, but enabling them will break compliance with FIPS 140-2. For more information, refer to the **FIPS 140-2 Non-Proprietary Security Policy** or contact Siemens Customer Support.*

• **Cyber Security Features**

Cyber security is an urgent issue in many industries where advanced automation and communications networks play a crucial role in mission critical applications and where high reliability is of paramount importance. Key RUGGEDCOM ROS features that address security issues at the local area network level include:

<b>Passwords</b>	Multi-level user passwords secures against unauthorized configuration
<b>SSH/SSL</b>	Extends capability of secure device management through secure methods of authentication, encryption and data integrity
<b>Enable/Disable Ports</b>	Capability to disable ports so that traffic cannot pass
<b>802.1Q VLAN</b>	Provides the ability to logically segregate traffic between predefined ports on switches
<b>HTTPS</b>	For secure access to the Web interface

• **Enhanced Rapid Spanning Tree Protocol (eRSTP)<sup>™</sup>**

Siemens's eRSTP allows the creation of fault-tolerant ring and mesh Ethernet networks that incorporate redundant links that are *pruned* to prevent loops. eRSTP implements both STP and RSTP to promote interoperability with commercial switches, unlike other proprietary *ring* solutions. The fast root failover feature of eRSTP provides quick network convergence in case of an RSTP root bridge failure in a mesh topology.

• **Quality of Service (IEEE 802.1p)**

Some networking applications such as real-time control or VoIP (Voice over IP) require predictable arrival times for Ethernet frames. Switches can introduce latency in times of heavy network traffic due to the internal queues that buffer frames and then transmit on a first come first serve basis. RUGGEDCOM ROS supports *Class of Service*, which allows time critical traffic to jump to the front of the queue, thus minimizing latency and reducing *jitter* to allow such demanding applications to operate correctly. RUGGEDCOM ROS allows priority classification by port, tags, MAC address, and IP Type of Service (ToS). A configurable *weighted fair queuing* algorithm controls how frames are emptied from the queues.

• **VLAN (IEEE 802.1Q)**

Virtual Local Area Networks (VLAN) allow the segregation of a physical network into separate logical networks with independent broadcast domains. A measure of security is provided since hosts can only access other hosts on the same VLAN and traffic storms are isolated. RUGGEDCOM ROS supports 802.1Q tagged Ethernet frames and VLAN trunks. Port based classification allows legacy devices to be assigned to the correct VLAN. GVRP support is also provided to simplify the configuration of the switches on the VLAN.

• **Simple Network Management Protocol (SNMP)**

When enabled, SNMP provides a standardized method, for network management stations, to interrogate devices from different vendors. SNMP versions include v1, v2c and v3. SNMPv3 in particular provides security features (such as authentication, privacy, and access control) not present in earlier SNMP versions. Numerous standard MIBs (Management Information Base) allow for easy integration with any Network Management System (NMS). A feature of SNMP supported by RUGGEDCOM ROS is the ability to generate *traps* upon system events. RUGGEDCOM NMS, the Siemens management solution, can record traps from multiple devices providing a powerful network troubleshooting tool. It also provides a graphical visualization of the network and is fully integrated with all Siemens products.

• **NTP (Network Time Protocol)**

NTP automatically synchronizes the internal clock of all RUGGEDCOM ROS devices on the network. This allows for correlation of time stamped events for troubleshooting.

- **Port Rate Limiting**  
RUGGEDCOM ROS supports configurable rate limiting per port to limit unicast and multicast traffic. This can be essential to managing precious network bandwidth for service providers. It also provides edge security for Denial of Service (DoS) attacks.
- **Broadcast Storm Filtering**  
Broadcast storms wreak havoc on a network and can cause attached devices to malfunction. This could be disastrous on a network with mission critical equipment. RUGGEDCOM ROS limits this by filtering broadcast frames with a user-defined threshold.
- **Link Aggregation**  
Ethernet ports can be aggregated into a single logical link either statically or dynamically to increase bandwidth and balance the traffic load.
- **Port Mirroring**  
RUGGEDCOM ROS can be configured to duplicate all traffic on one port to a designated mirror port. When combined with a network analyzer, this can be a powerful troubleshooting tool.
- **Port Configuration and Status**  
RUGGEDCOM ROS allows individual ports to be *hard* configured for speed, duplex, auto-negotiation, flow control and more. This allows proper connection with devices that do not negotiate or have unusual settings. Detailed status of ports with alarm and SNMP trap on link problems aid greatly in system troubleshooting.
- **Port Statistics and RMON (Remote Monitoring)**  
RUGGEDCOM ROS provides continuously updating statistics per port that provide both ingress and egress packet and byte counters, as well as detailed error figures.  
  
Also provided is full support for RMON statistics. RMON allows for very sophisticated data collection, analysis and detection of traffic patterns.
- **Multicast Filtering**  
RUGGEDCOM ROS supports static multicast groups and the ability to join or leave multicast groups dynamically using IGMP (Internet Group Management Protocol) or GMRP (GARP Multicast Registration Protocol).
- **Event Logging and Alarms**  
RUGGEDCOM ROS records all significant events to a non-volatile system log allowing forensic troubleshooting. Events include link failure and recovery, unauthorized access, broadcast storm detection, and self-test diagnostics among others. Alarms provide a snapshot of recent events that have yet to be acknowledged by the network administrator. An external hardware relay is de-energized during the presence of critical alarms, allowing an external controller to react if desired.
- **HTML Web Browser User Interface**  
RUGGEDCOM ROS provides a simple, intuitive user interface for configuration and monitoring via a standard graphical Web browser or via a standard telcom user interface. All system parameters include detailed online help to facilitate setup and configuration. RUGGEDCOM ROS presents a common look and feel and standardized configuration process, allowing easy migration to other managed RUGGEDCOM products.

## Section 1.2

## Security Recommendations

To prevent unauthorized access to the device, note the following security recommendations:

**IMPORTANT!**

*The following insecure protocols are disabled by default in RUGGEDCOM ROS: RADIUS, TACACS+, RSH, Telnet, TFTP, ModBus management, Remote Syslog, SNMPv1, SNMPv2 and SNMPv3. To meet varied customer needs, these protocols can be enabled, but enabling them will break compliance with FIPS*

140-2. For more information, refer to the **FIPS 140-2 Non-Proprietary Security Policy** or contact Siemens Customer Support.

## » Authentication

- Replace the default passwords for all user accounts and processes (where applicable) before the device is deployed.
- Use strong passwords with high randomization (i.e. entropy), without repetition of characters. Avoid weak passwords such as *password1*, *123456789*, *abcdefgh*, and any dictionary words or proper names in any combination. For more information about creating strong passwords, refer to the password requirements in [Section 6.1.1, "Configuring Passwords"](#).
- Make sure passwords are protected and not shared with unauthorized personnel.
- Passwords should not be re-used across different user names and systems, or after they expire.
- If RADIUS authentication is done remotely, make sure all communications are within the security perimeter or on a secure channel.
- Generate and provision a custom SSL certificate and SSH host key pair before commissioning the device. For more information, refer to [Section 6.5, "Managing SSH and SSL Keys and Certificates"](#).
- Use SSH public key authentication. For more information, refer to [Section 6.5, "Managing SSH and SSL Keys and Certificates"](#).

## » Physical/Remote Access

- Do not connect the device to the Internet. Deploy the device only within a secure network perimeter.
- Restrict physical access to the device to only authorized personnel. A person with malicious intent could extract critical information, such as private keys, (user passwords are protected by hash codes), or reprogram the device.
- Only enable services that will be used on the device, including physical ports. Unused physical ports could potentially be used to gain access to the network behind the device.
- If SNMP is enabled, limit the number of IP addresses that can connect to the device and change the community names. Also configure SNMP to raise a trap upon authentication failures. For more information, refer to [Section 10.2, "Managing SNMP"](#).
- Avoid using insecure services such as Telnet and TFTP, or disable them completely if possible. These services are available for historical reasons and are disabled by default.
- Limit the number of simultaneous Web Server, Telnet and SSH sessions allowed.
- Configure remote system logging to forward all logs to a central location. For more information, refer to [Section 4.5, "Managing Logs"](#).
- Configuration files are provided in the CSV (comma separated values) format for ease of use. Make sure configuration files are properly protected when they exist outside of the device. For instance, encrypt the files, store them in a secure place, and do not transfer them via insecure communication channels.
- Be aware of any non-secure protocols enabled on the device. While some protocols, such as HTTPS and SSH, are secure, others, such as Telnet and RSH, were not designed for this purpose. Appropriate safeguards against non-secure protocols should be taken to prevent unauthorized access to the device/network.
- Configure port security features on access ports to prevent an unauthorized third-party from physically connecting to the device. For more information, refer to [Section 6.4, "Managing Port Security"](#).

## » Hardware/Software

- Make sure the latest firmware version is installed, including all security-related patches. For the latest information on security patches for Siemens products, visit the [Industrial Security website](https://www.siemens.com/global/en/home/company/topic-areas/future-of-manufacturing/industrial-security.html) [https://www.siemens.com/global/en/home/company/topic-areas/future-of-manufacturing/industrial-security.html] or the [ProductCERT Security Advisories website](http://www.siemens.com/innovation/en/technology-focus/siemens-cert/cert-security-advisories.htm) [http://www.siemens.com/innovation/en/technology-focus/siemens-cert/cert-security-advisories.htm]. Updates to Siemens Product Security Advisories can be obtained by subscribing to the RSS feed on the Siemens ProductCERT Security Advisories website, or by following @ProductCert on Twitter.
- Enable BPDU Guard on ports where RSTP BPDUs are not expected.
- Use the latest Web browser version compatible with RUGGEDCOM ROS to make sure the most secure Transport Layer Security (TLS) versions and ciphers available are employed.
- Modbus management interface is insecure and is disabled by default in RUGGEDCOM ROS. When enabled, compliance with FIPS will be broken. If Modbus management interface is required, then it is recommended to follow the security recommendations outlined in this User Guide and to configure the environment according to defense-in-depth best practices.
- Prevent access to external, untrusted Web pages while accessing the device via a Web browser. This can assist in preventing potential security threats, such as session hijacking.
- For optimal security, use SNMPv3 whenever possible. Use strong authentication keys and private keys without repetitive strings ( e.g. *abc* or *abcabc*) with this feature. For more information about creating strong passwords, refer to the password requirements in [Section 6.1.1, "Configuring Passwords"](#).
- Unless required for a particular network topology, the *IP Forward* setting should be set to `Disabled` to prevent the routing of packets.

## » Policy

- Periodically audit the device to make sure it complies with these recommendations and/or any internal security policies.
- Review the user documentation for other Siemens products used in coordination with device for further security recommendations.

### Section 1.3

## Supported Networking Standards

The following networking standards are supported by RUGGEDCOM ROS:

Standard	10 Mbps Ports	100 Mbps Ports	1000 Mbps Ports	Notes
IEEE 802.3x	✓	✓	✓	Full Duplex Operation
IEEE 802.3z			✓	1000Base-LX
IEEE 802.3ab			✓	1000Base-Tx
IEEE 802.1D	✓	✓	✓	MAC Bridges
IEEE 802.1Q	✓	✓	✓	VLAN (Virtual LAN)
IEEE 802.1p	✓	✓	✓	Priority Levels

Section 1.4

# Port Numbering Scheme

For quick identification, each port on a RUGGEDCOM RS900GPF device is assigned a number. All port numbers are silk-screened on the device.

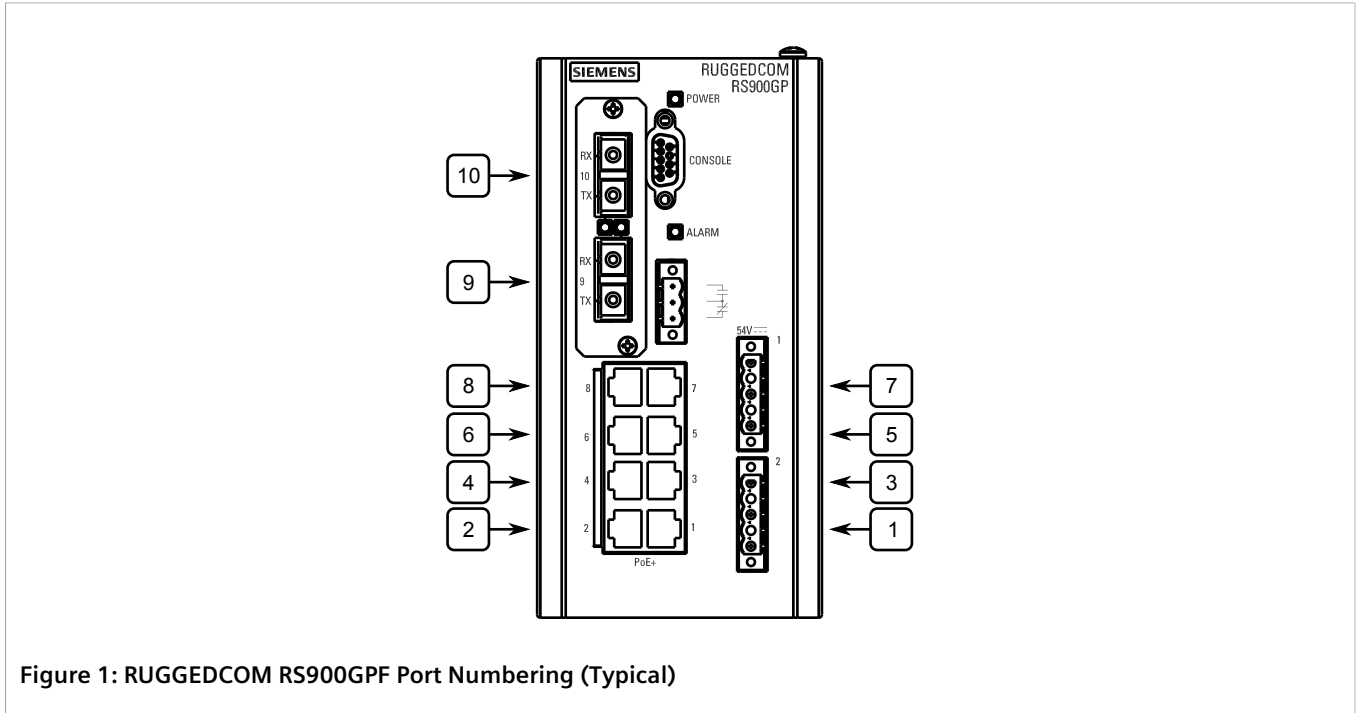


Figure 1: RUGGEDCOM RS900GPF Port Numbering (Typical)

Use these numbers to configure applicable features on select ports.

Section 1.5

# Available Services by Port

The following table lists the services available under RUGGEDCOM ROS. This table includes the following information:



### IMPORTANT!

The following insecure protocols are disabled by default in RUGGEDCOM ROS: RADIUS, TACACS+, RSH, Telnet, TFTP, ModBus management, Remote Syslog, SNMPv1, SNMPv2 and SNMPv3. To meet varied customer needs, these protocols can be enabled, but enabling them will break compliance with FIPS 140-2. For more information, refer to the **FIPS 140-2 Non-Proprietary Security Policy** or contact Siemens Customer Support.

- **Services**  
The service supported by the device.
- **Port Number**  
The port number associated with the service.
- **Port Open**  
The port state, whether it is always open and cannot be closed, or open only, but can be configured.



**NOTE**

*In certain cases, the service might be disabled, but the port can still be open (e.g. TFTP).*

- **Port Default**

The default state of the port (i.e. open or closed).

- **Access Authorized**

Denotes whether the ports/services are authenticated during access.

Services	Port Number	Service Enabled/ Disabled	Access Authorized	Note
Telnet	TCP/23	Disabled	Yes	Only available through management interfaces.
HTTP	TCP/80	Enabled (configurable), redirects to 443	—	
HTTPS	TCP/443	Enabled (configurable)	Yes	
RSH	TCP/514	Disabled (configurable)	Yes	Only available through management interfaces.
TFTP	UDP/69	Disabled (configurable)	No	Only available through management interfaces.
SFTP	TCP/22	Enabled	Yes	Only available through management interfaces.
SNMP	UDP/161	Disabled (configurable)	Yes	Only available through management interfaces.
SNTP	UDP/123	Enabled (configurable)	No	Only available through management interfaces.
SSH	TCP/22	Enabled	Yes	Only available through management interfaces.
ICMP	—	Enabled	No	
TACACS+	TCP/49 (configurable)	Disabled (configurable)	Yes	
RADIUS	UDP/1812 to send (configurable), opens random port to listen to	Disabled (configurable)	Yes	Only available through management interfaces.
Remote Syslog	UDP/514 (configurable)	Disabled (configurable)	No	Only available through management interfaces.
TCP Modbus (Server)	TCP/502	Disabled (configurable)	No	Only available through management interfaces.
TCP Modbus (Switch)	TCP/502	Disabled (configurable)	No	
DHCP, DHCP Agent	UDP/67, 68 sending msg if enabled - if received, always come to CPU, dropped if service not configured	Disabled (configurable)	No	

Section 1.6

# FIPS Self-Tests

FIPS self-tests are performed automatically by RUGGEDCOM ROS in compliance with FIPS standards. Power up self-tests are performed during bootup, and runtime tests are performed during normal operation.

The following sections describe the self-tests being performed, and outlines a procedure to manually launch the FIPS cryptographic algorithm self-tests.

## CONTENTS

- [Section 1.6.1, "FIPS Power Up Self-Tests"](#)
- [Section 1.6.2, "FIPS Runtime Tests"](#)
- [Section 1.6.3, "Manually Launching FIPS Cryptographic Algorithm Tests"](#)

Section 1.6.1

## FIPS Power Up Self-Tests

Power up self-tests are performed automatically during the boot sequence. Tests include a firmware integrity test, cryptographic algorithm self-tests, and entropy tests. The cryptographic functions are available only after all power up self-tests pass successfully.

As tests pass, a *test passed* message is written to the system log file (`syslog.txt`).

If one of the power up self-tests fails, the following occurs:

1. The failure event is written to the system log file (`syslog.txt`), similar to **{test} failed**, where *{test}* is the name of the failed test, or **Cryptographic tests failed. {error code} » {algorithm} test failed!**, where *{error code}* is the generated error code and *{algorithm}* is the name of the failed algorithm.
2. The alarm indicator LED (if equipped) blinks five times.
3. The device is restarted.

A self-test failure is most likely due to an unexpected hardware fault or unauthorized physically tampering. In order to account for potential faults triggered by external conditions, the system will continue to attempt to boot and clear all the self-tests. If, however, ten failures are logged within a one-hour period, the system will transition to maintenance mode. For more information about maintenance mode, refer to [Section 2.8, "Accessing Maintenance Mode"](#).

The following tests are performed as part of the FIPS power up self-test process:

- **Firmware Integrity Test**

The firmware integrity test uses an SHA-256 digest to make sure the firmware binary image has not been corrupted.

- **Cryptographic Algorithm Tests**

Cryptographic algorithm tests verify if all cryptographic algorithms are operating correctly. All cryptographic algorithm test results are stored by the device for the run-time tests verification. Cryptographic algorithms tests include a set of known-answer tests (KATs) and pair-wise consistency tests (PCTs).



### NOTE

A list of the specific cryptographic tests can be displayed by typing `crypttest list` at a CLI prompt.



Selective and advanced invocation of certain cryptographic algorithm tests is supported. For more information, refer to the *FIPS 140-2 Non-Proprietary Security Policy* or contact Siemens Customer Support.

- **Entropy Tests**

Entropy tests verify the entropy collection mechanism is working correctly at power up. The collected entropy is stored in the internal entropy pool. Entropy tests include the following:

- Repetition test
- Adaptive proportion test
- Arithmetic mean value test
- Entropy value test
- Stuck-at-constant-failure test

### Section 1.6.2

## FIPS Runtime Tests

Runtime tests are performed during normal operation of RUGGEDCOM ROS.

If one of the runtime tests fails, the following occurs:

1. The failure event is written to the system log file (`syslog.txt`).
2. The alarm indicator LED (if equipped) blinks five times.
3. All open files are closed.
4. The database is closed.
5. The device is restarted.

If no resolution is found after ten attempts, the device automatically reboots into maintenance mode. For more information about maintenance mode, refer to [Section 2.8, "Accessing Maintenance Mode"](#).

Runtime tests include the following:

Type	Test(s)	Log Message on Failure
Entropy	Stuck-at-constant-failure test	Entropy collection failed
DRBG	Stuck-at-constant-failure test, powerup self-tests status verification	DRBG return error: ERR_FIPS_CTRDRBG_FAIL
Cryptographic Algorithm	RSA pairwise consistency test, EC Diffie-Hellman public key assurance test	Failed to <b>{description}</b> , where <i>{description}</i> is the algorithm usage description

### Section 1.6.3

## Manually Launching FIPS Cryptographic Algorithm Tests

Although cryptographic algorithm self-tests are performed automatically during module power up, they can also be manually launched on demand.

To launch cryptographic algorithm self-tests, do the following:

1. Log in to the device as an admin user and access the CLI shell. For more information about accessing the CLI shell, refer to [Section 2.5, "Using the Command Line Interface"](#).
2. At the CLI prompt, type:

**factory**

3. When prompted, answer yes and enter the password.
4. At the CLI prompt, type:

**cryptest**

Running the **cryptest** command with no other arguments begins running each self-test in sequence as described in [Section 1.6, "FIPS Self-Tests"](#).

If all tests pass, the following message appears:

```
Cryptographic algorithm self tests passed
```

If one of the power up self-tests fails, the device will follow the sequence described in [Section 1.6.1, "FIPS Power Up Self-Tests"](#), and may eventually reboot into maintenance mode. For more information about maintenance mode, refer to [Section 2.8, "Accessing Maintenance Mode"](#).



**NOTE**

*Booting into maintenance mode will automatically delete the `ssl.crt`, `ssh.keys` and `config.csv` files.*

# 2 Using ROS

This chapter describes how to use RUGGEDCOM ROS.

## CONTENTS

- [Section 2.1, "Logging In"](#)
- [Section 2.2, "Logging Out"](#)
- [Section 2.3, "Using the Web Interface"](#)
- [Section 2.4, "Using the Console Interface"](#)
- [Section 2.5, "Using the Command Line Interface"](#)
- [Section 2.6, "Selecting Ports in RUGGEDCOM ROS"](#)
- [Section 2.7, "Managing the Flash File System"](#)
- [Section 2.8, "Accessing Maintenance Mode"](#)

## Section 2.1

# Logging In

To log in to the device, do the following:

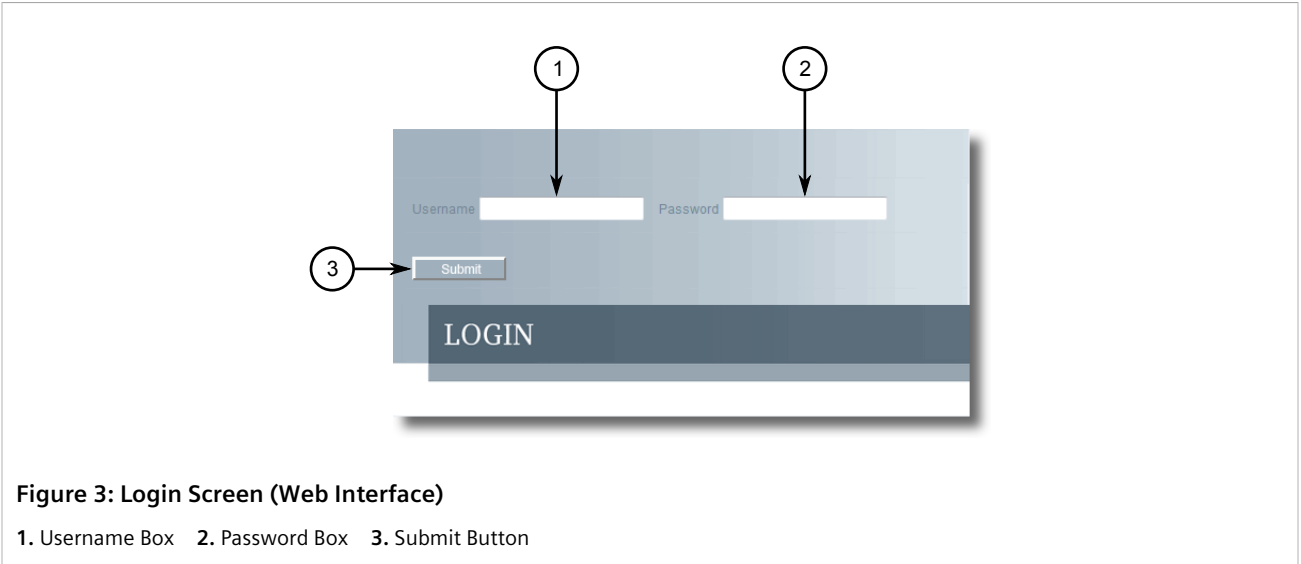
1. Connect to the device either directly or through a Web browser. For more information about how to connect to the device, refer to [Section 3.1, "Connecting to ROS"](#).

Once the connection is established, the login form appears.



**Figure 2: SSH Login Screen (Console Interface)**

1. User Name Box 2. Password Box



**Figure 3: Login Screen (Web Interface)**

1. Username Box 2. Password Box 3. Submit Button



**NOTE**

*The following default user names and passwords are set on the device for each user type:*

**Guest**

*User Name: guest*

*Password: guest*

**Operator**

*User Name: operator*

*Password: operator*

**Admin**

*User Name: admin*

*Password: admin*



**CAUTION!**

*To prevent unauthorized access to the device, make sure to change the default guest, operator, and admin passwords before commissioning the device.*

*For more information about changing passwords, refer to [Section 6.1.1, "Configuring Passwords"](#).*

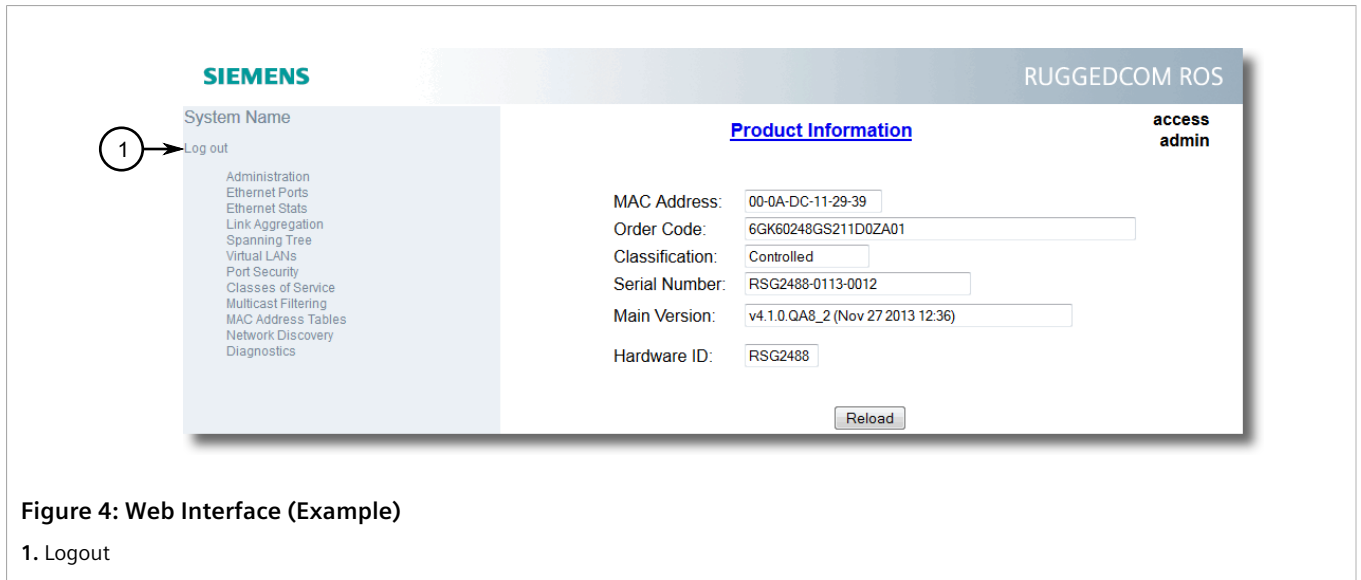
2. In the **User Name** field, type the user name for an account setup on the device.
3. In the **Password** field, type the password for the account.
4. Click **Enter** or click **Submit** (Web interface only).

Section 2.2

## Logging Out

To log out of the device, navigate to the main screen and do the following:

- To log out of the Console or secure shell interfaces, press **CTRL + X**.
- To log out of the Web interface, click **Logout**.



**Figure 4: Web Interface (Example)**

1. Logout



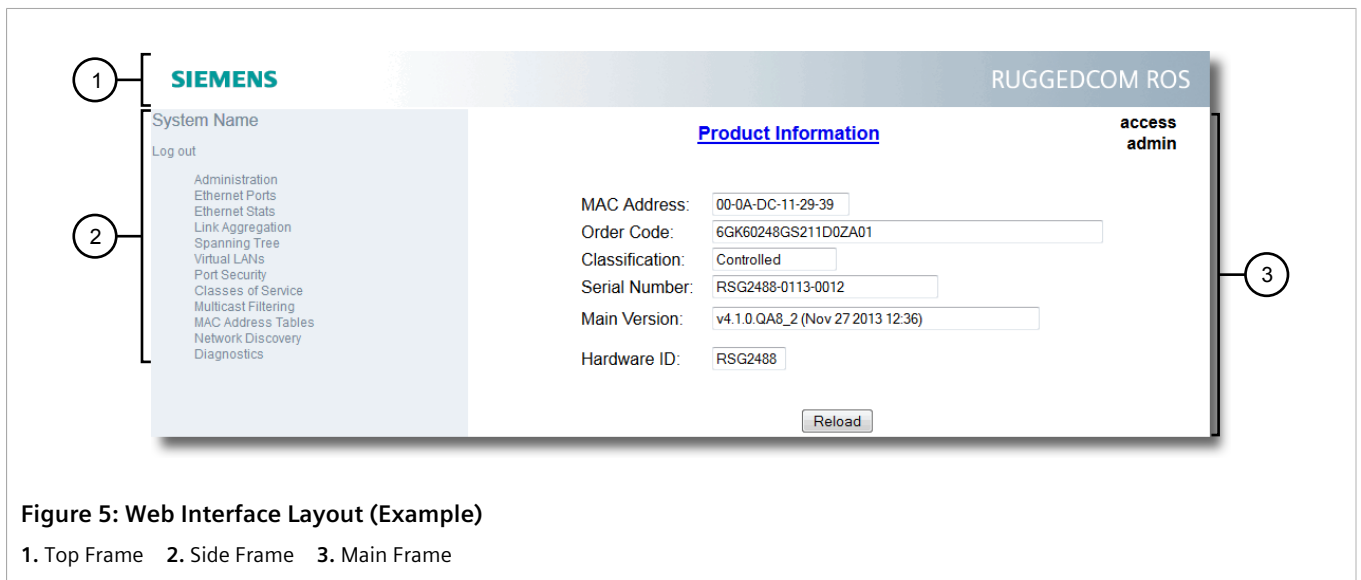
**NOTE**

*If any pending configuration changes have not been committed, RUGGEDCOM ROS will request confirmation before discarding the changes and logging out of the device.*

Section 2.3

# Using the Web Interface

The Web interface is a Web-based Graphical User Interface (GUI) for displaying important information and controls in a Web browser. The interface is divided into three frames: the banner, the menu and the main frame.



**Figure 5: Web Interface Layout (Example)**

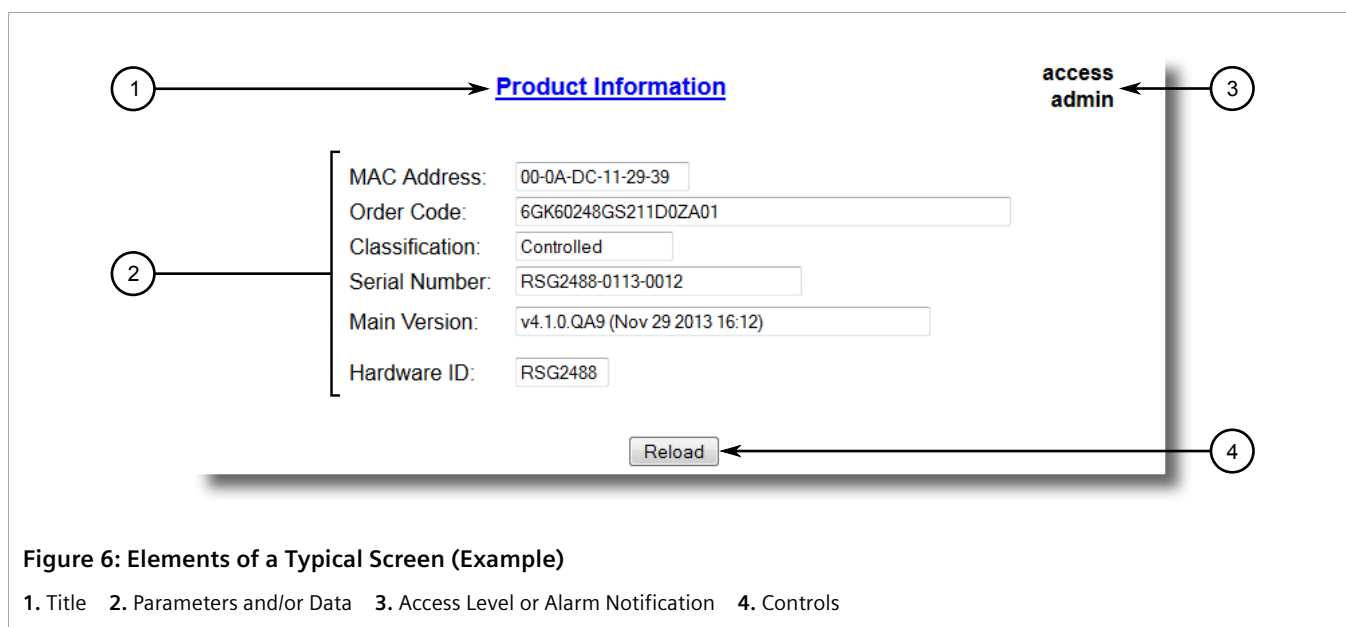
1. Top Frame 2. Side Frame 3. Main Frame

Frame	Description
Top	The top frame displays the system name for the device.

Frame	Description
Side	The side frame contains a logout option and a collapsible list of links that open various screens in the main frame. For information about logging out of RUGGEDCOM ROS, refer to <a href="#">Section 2.2, "Logging Out"</a> .
Main	The main frame displays the parameters and/or data related to the selected feature.

Each screen consists of a title, the current user's access level, parameters and/or data (in form or table format), and controls (e.g. add, delete, refresh, etc.). The title provides access to context-specific Help for the screen that provides important information about the available parameters and/or data. Click on the link to open the Help information in a new window.

When an alarm is generated, an alarm notification replaces the current user's access level on each screen until the alarm is cleared. The notification indicates how many alarms are currently active. For more information about alarms, refer to [Section 5.4, "Managing Alarms"](#).



**Figure 6: Elements of a Typical Screen (Example)**

1. Title 2. Parameters and/or Data 3. Access Level or Alarm Notification 4. Controls



**NOTE**

*If desired, the web interface can be disabled. For more information, refer to [Section 5.3, "Enabling/Disabling the Web Interface"](#).*

Section 2.4

## Using the Console Interface

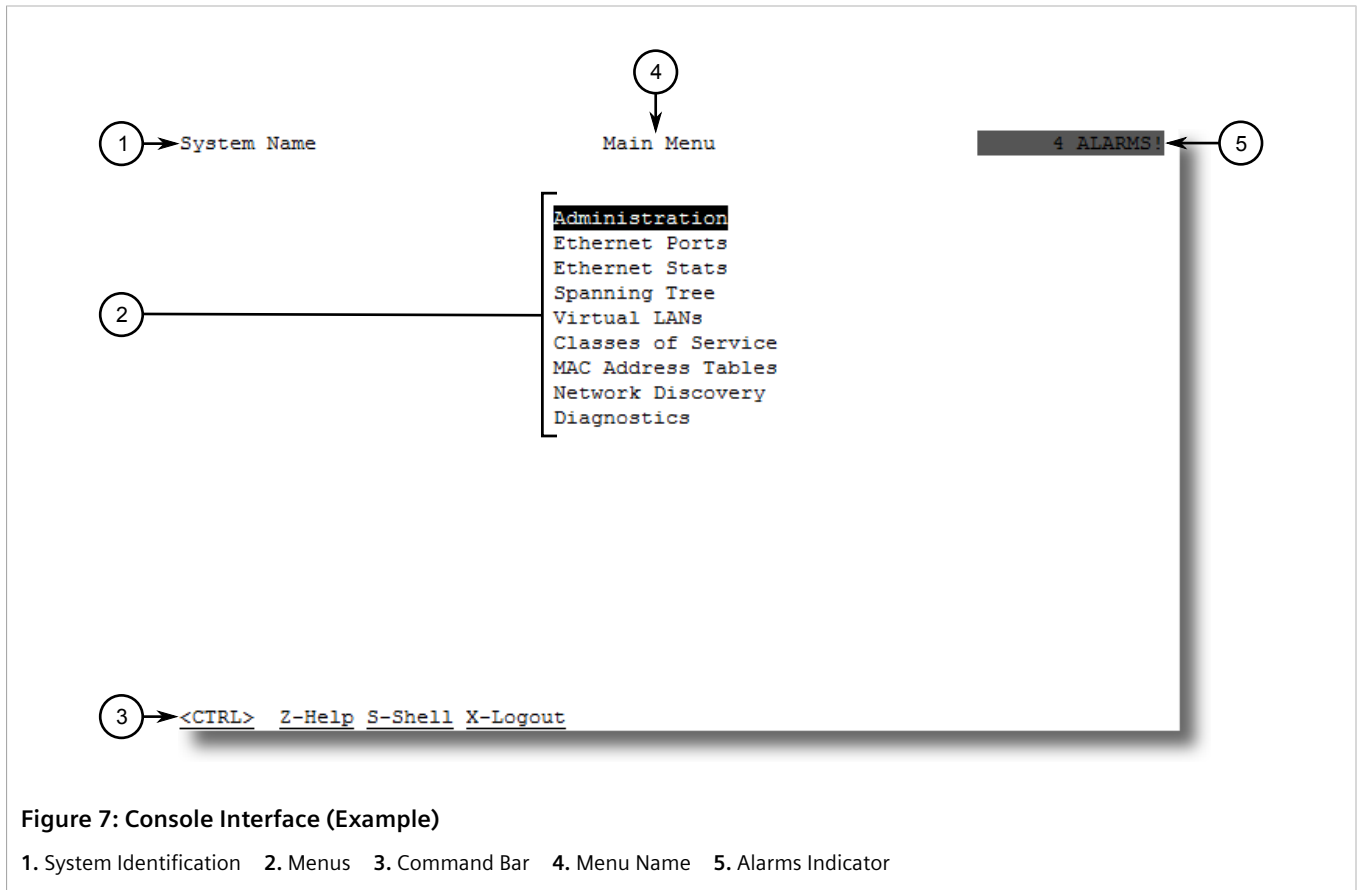
The Console interface is a Graphical User Interface (GUI) organized as a series of menus. It is primarily accessible through a serial console connection, but can also be accessed through IP services, such as a Telnet, RSH (Remote Shell), SSH (Secure Shell) session, or SSH remote command execution.



**NOTE**

*IP services can be restricted to control access to the device. For more information, refer to [Section 4.10, "Configuring IP Services"](#).*

Each screen consists of a system identifier, the name of the current menu, and a command bar. Alarms are also indicated on each screen in the upper right corner.



**NOTE**  
 The system identifier is user configurable. For more information about setting the system name, refer to [Section 5.1, "Configuring the System Information"](#).

### » Navigating the Interface

Use the following controls to navigate between screens in the Console interface:

Enter	Select a menu item and press this <b>Enter</b> to enter the sub-menu or screen beneath.
Esc	Press <b>Esc</b> to return to the previous screen.


### » Configuring Parameters

Use the following controls to select and configure parameters in the Console interface:

Up/Down Arrow Keys	Use the up and down arrow keys to select parameters.
Enter	Select a parameter and press <b>Enter</b> to start editing a parameter. Press <b>Enter</b> again to commit the change.
Esc	When editing a parameter, press <b>Esc</b> to abort all changes.

## » Commands

The command bar lists the various commands that can be issued in the Console interface. Some commands are specific to select screens. The standard commands include the following:

<b>Ctrl + A</b>	Commits configuration changes made on the current screen.
	<div style="border: 1px solid gray; padding: 5px;">  <b>NOTE</b>  <i>Before exiting a screen, RUGGEDCOM ROS will automatically prompt the user to save any changes that have not been committed.</i> </div>
<b>Ctrl + I</b>	Inserts a new record.
<b>Ctrl + L</b>	Deletes a record.
<b>Ctrl + S</b>	Opens the CLI interface.
<b>Ctrl + X</b>	Terminates the current session. This command is only available from the main menu.
<b>Ctrl + Z</b>	Displays important information about the current screen or selected parameter.

### Section 2.5

## Using the Command Line Interface

The Command Line Interface (CLI) offers a series of powerful commands for updating RUGGEDCOM ROS, generating certificates/keys, tracing events, troubleshooting and much more. It is accessed via the Console interface by pressing **Ctrl-S**.

### CONTENTS

- [Section 2.5.1, "Available CLI Commands"](#)
- [Section 2.5.2, "Tracing Events"](#)
- [Section 2.5.3, "Executing Commands Remotely via RSH"](#)
- [Section 2.5.4, "Executing Secure Commands Remotely via SSH"](#)
- [Section 2.5.5, "Using SQL Commands"](#)


### Section 2.5.1

## Available CLI Commands

The following commands are available at the command line:

Command	Description	Authorized Users
<b>alarms</b> <i>all</i>	Displays a list of available alarms. Optional and/or required parameters include: <ul style="list-style-type: none"> <li>• <i>all</i> displays all available alarms</li> </ul>	Guest, Operator, Admin
<b>arp</b>	Displays the IP to MAC address resolution table.	Admin
<b>clearalarms</b>	Clears all alarms.	Operator, Admin
<b>clearethstats</b> [ <i>all</i>   <i>port</i> ]	Clears Ethernet statistics for one or more ports. Optional and/or required parameters include:	Operator, Admin



Command	Description	Authorized Users
	<ul style="list-style-type: none"> <li>• <code>all</code> clears statistics for all ports</li> <li>• <code>port</code> is a comma separated list of port numbers (e.g. 1,3-5,7)</li> </ul>	
<code>clearlogs</code>	Clears the system and crash logs.	Admin
<code>clearmgmtstats</code>	Clear statistics for Ethernet Mgmt port.	Admin
<code>clksyn</code>	Clock Synthesizer diagnostics.	Admin
<code>clrcblstats</code> [ <code>all</code>   <code>port</code> ]	Clears cable diagnostics statistics for one or more ports. Optional and/or required parameters include: <ul style="list-style-type: none"> <li>• <code>all</code> clears statistics for all ports</li> <li>• <code>port</code> is a comma separated list of port numbers (e.g. 1,3-5,7)</li> </ul>	Admin
<code>clrstpstats</code>	Clears all spanning tree statistics.	Operator, Admin
<code>cls</code>	Clears the screen.	Guest, Operator, Admin
<code>cryptest</code>	Executes cryptographic algorithm self tests.	Admin
<code>diag</code>	Block Cipher Mode (BCM) diagnostic shell commands.	Admin
<code>dir</code>	Prints the directory listing.	Guest, Operator, Admin
<code>docsummary</code>	Print all fields in the database that are configurable.	Admin
<code>eeeprom</code>	EEPROM memory diagnostic commands.	Admin
<code>exit</code>	Terminates the session.	Guest, Operator, Admin
<code>factory</code>	<p>Enables factory mode, which includes several factory-level commands used for testing and troubleshooting. Only available to admin users.</p> <div style="border: 1px solid black; padding: 5px; background-color: #f0f0f0;">  <p><b>CAUTION!</b> Misuse of the factory commands may corrupt the operational state of device and/or may permanently damage the ability to recover the device without manufacturer intervention.</p> </div>	Admin
<code>flashfiles</code> { <code>info filename</code>   <code>defrag</code> }	<p>A set of diagnostic commands to display information about the Flash filesystem and to defragment Flash memory.</p> <p>Optional and/or required parameters include:</p> <ul style="list-style-type: none"> <li>• <code>info filename</code> displays information about the specified file in the Flash file system</li> <li>• <code>defrag</code> defragments files in the Flash file system</li> </ul> <p>For more information about the <b>flashfiles</b> command, refer to <a href="#">Section 2.7, "Managing the Flash File System"</a>.</p>	Admin
<code>flashleds</code> <code>timeout</code>	<p>Flashes the LED indicators on the device for a specified number of seconds.</p> <p>Optional and/or required parameters include:</p> <ul style="list-style-type: none"> <li>• <code>timeout</code> is the number of seconds to flash the LED indicators. To stop the LEDs from flashing, set the timeout period to 0 (zero).</li> </ul>	Admin
<code>fpgacmd</code>	Provides access to the FPGA management tool for troubleshooting time synchronization.	Admin
<code>hashInfo</code>	Displays Hash table information.	Admin
<code>help</code> <code>command</code>	Displays a brief description of the specified command. If no command is specified, it displays a list of all available commands, including a description for each.	Guest, Operator, Admin

Command	Description	Authorized Users
	Optional and/or required parameters include: <ul style="list-style-type: none"> <li><i>command</i> is the command name.</li> </ul>	
<code>i2c0</code>	Read/Write via I2C.	Admin
<code>i2c1</code>	Read/Write via I2C.	Admin
<code>ipconfig</code>	Displays the current IP address, subnet mask and default gateway. This command provides the only way of determining these values when DHCP is used.	Guest, Operator, Admin
<code>klog</code>	Controls the MQX kernel log service.	Admin
<code>loadflts</code>	Loads the factory default configuration.	Admin
<code>logout</code>	Logs out of the shell.	Guest, Operator, Admin
<code>logs</code>	Displays syslog entries in CLI shell.	Admin
<code>lp</code>	Reads and displays LED panel control registers.	Admin
<code>maintenance</code>	Enter maintenance mode.	Admin
<code>ping address { count   timeout }</code>	<p>Sends an ICMP echo request to a remotely connected device. For each reply received, the round trip time is displayed. Use this command to verify connectivity to the next connected device. It is a useful tool for testing commissioned links. This command also includes the ability to send a specific number of pings with a specified time for which to wait for a response.</p> <p>Optional and/or required parameters include:</p> <ul style="list-style-type: none"> <li><i>address</i> is the target IP address.</li> <li><i>count</i> is the number of echo requests to send. The default is 4.</li> <li><i>timeout</i> is the time in milliseconds to wait for each reply. The range is 2 to 5000 seconds. The default is 300 milliseconds.</li> </ul> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p><b>NOTE</b>  <i>The device to be pinged must support ICMP echo. Upon commencing the ping, an ARP request for the MAC address of the device is issued. If the device to be pinged is not on the same network as the device pinging the other device, the default gateway must be programmed.</i></p> </div>	Guest, Operator, Admin
<code>portpin</code>	View and control I/O pins.	Admin
<code>psclog</code>	Clear data log in power supply board.	Admin
<code>psseq</code>	Power Supply Sequencer Register diagnostics.	Admin
<code>purgemac</code>	Purges the MAC Address table.	Operator, Admin
<code>random</code>	Display seeds or random numbers.	Admin
<code>reset</code>	Perform a hard reset of the switch.	Operator, Admin
<code>resetport { all   ports }</code>	<p>Resets one or more Ethernet ports, which may be useful for forcing re-negotiation of speed and duplex, or in situations where the link partner has latched into an inappropriate state.</p> <p>Optional and/or required parameters include:</p> <ul style="list-style-type: none"> <li><i>all</i> resets all ports</li> <li><i>ports</i> is a comma separated list of port numbers (e.g. 1,3-5,7)</li> </ul>	Operator, Admin
<code>rmon</code>	Displays the names of all RMON alarm eligible objects.	Guest, Operator, Admin

Command	Description	Authorized Users
<b>route</b>	Displays the gateway configuration.	Guest, Operator, Admin
<b>rtc</b>	Real-Time Clock Register diagnostics.	Admin
<b>sfp</b> <i>port</i> { <i>base</i>   <i>alarms</i>   <i>diag</i>   <i>calibr</i>   <i>thr</i>   <i>all</i>   <i>no parameter specified</i> }	Displays SFP (Small Form Factor Pluggable) device information and diagnostics. If optional or required parameters are not used, this command displays the base and extended information. Optional and/or required parameters include: <ul style="list-style-type: none"> <li>• <i>port</i> is the port number for which the data are required</li> <li>• <i>base</i> displays the base information</li> <li>• <i>alarms</i> displays alarms and warning flags</li> <li>• <i>diag</i> displays measured data</li> <li>• <i>calibr</i> displays calibration data for external calibration</li> <li>• <i>thr</i> displays thresholds data</li> <li>• <i>all</i> displays all diagnostic data</li> </ul>	Admin
<b>smi</b>	SMI interface diagnostics.	Admin
<b>spi</b>	Read/Write via SPI.	Admin
<b>spuriouscount</b>	Displays user spurious interrupt count.	Admin
<b>sql</b> { <i>default</i>   <i>delete</i>   <i>help</i>   <i>info</i>   <i>insert</i>   <i>save</i>   <i>select</i>   <i>update</i> }	Provides an SQL-like interface for manipulating all system configuration and status parameters. All commands, clauses, table, and column names are case insensitive. Optional and/or required parameters include: <ul style="list-style-type: none"> <li>• <i>default</i> sets all records in a table(s) to factory defaults</li> <li>• <i>delete</i> allows for records to be deleted from a table</li> <li>• <i>help</i> provides a brief description for any SQL command or clause</li> <li>• <i>info</i> displays a variety of information about the tables in the database</li> <li>• <i>insert</i> enables new records to be inserted into a table</li> <li>• <i>save</i> saves the database to non-volatile memory storage</li> <li>• <i>select</i> queries the database and displays selected records</li> <li>• <i>update</i> enable existing records in a table to be updated</li> </ul> For more information about the <b>sql</b> command, refer to <a href="#">Section 2.5.5, "Using SQL Commands"</a> .	Admin
<b>sshkeygen</b> <i>rsa</i> [ 2048   3072 ] <i>N</i>	Generates new SSH keys in <i>ssh.keys</i> . Keys can be either 2048 or 3072 bits long.	Admin
<b>sshpubkey</b>	List, remove and update key entries in <i>sshpublish.keys</i> file.	Admin
<b>statmon</b>	Monitor BCM statistic counters.	Admin
<b>telnet</b> <i>dest</i>	Opens a telnet session. Press <b>Ctrl-C</b> to close the session. Optional and/or required parameters include: <ul style="list-style-type: none"> <li>• <i>dest</i> is the server's IP address</li> </ul>	Guest, Operator, Admin
<b>tftp</b> <i>address</i> [ <i>put</i>   <i>get</i> ] <i>source target</i>	Opens a TFTP session. Press <b>Ctrl-C</b> to close the session. Optional and/or required parameters include: <ul style="list-style-type: none"> <li>• <i>address</i> is the IP address of the remote TFTP server</li> <li>• <i>put</i> indicates TFTP will be uploading the source file to replace the destination file</li> <li>• <i>get</i> indicates TFTP will be downloading the source file to replace the destination file</li> <li>• <i>source</i> is the name of the source file</li> </ul>	Admin

Command	Description	Authorized Users
	<ul style="list-style-type: none"> <li><code>target</code> is the name of the file that will be replaced</li> </ul>	
<code>trace</code>	Starts event tracing. Run <code>trace ?</code> for more help.	Operator, Admin
<code>tree</code>	Displays SNMP tree.	Admin
<code>type filename</code>	Displays the contents of a text file. Optional and/or required parameters include: <ul style="list-style-type: none"> <li><code>filename</code> is the name of the file to be read</li> </ul>	Guest, Operator, Admin
<code>version</code>	Prints the software version.	Guest, Operator, Admin
<code>watchdog</code>	Provides ability to test watchdog(s).	Admin
<code>xmodem { send   receive } filename</code>	Opens an XModem session. Optional and/or required parameters include: <ul style="list-style-type: none"> <li><code>send</code> sends the file to the client.</li> <li><code>receive</code> receives the file from the client.</li> <li><code>filename</code> is the name of the file to be read.</li> </ul>	Operator, Admin

## Section 2.5.2

## Tracing Events

The CLI trace command provides a means to trace the operation of various protocols supported by the device. Trace provides detailed information, including STP packet decodes, IGMP activity and MAC address displays.

**NOTE**

*Tracing has been designed to provide detailed information to expert users. Note that all tracing is disabled upon device startup.*

To trace an event, do the following:

1. Log in to the device as an admin user and access the CLI shell. For more information about accessing the CLI shell, refer to [Section 2.5, "Using the Command Line Interface"](#).
2. Determine the protocols and associated options available by typing:

```
trace ?
```

If an option such as `allon` or `alloff` is required, determine which options are available for the desired protocol by typing:

```
trace protocol ?
```

**NOTE**

*If required, expand the trace scope by stringing protocols and their associated options together using a vertical bar (|).*

3. Select the type of trace to run by typing:

```
trace protocol option
```

Where:

- `protocol` is the protocol to trace
- `option` is the option to use during the trace

Example:

```
>trace transport allon
      TRANSPORT: Logging is enabled
```

4. Start the trace by typing:

```
trace
```

### Section 2.5.3

## Executing Commands Remotely via RSH

The Remote Shell (RSH) facility can be used from a workstation to cause the product to act upon commands as if they were entered at the CLI prompt. The syntax of the RSH command is usually of the form:

```
rsh ipaddr -l auth_token command_string
```

Where:

- *ipaddr* is the address or resolved name of the device.
- *auth\_token* is the user name (i.e. guest, operator or admin) and corresponding password separated by a comma. For example, *admin,secret*.
- *command\_string* is the RUGGEDCOM ROS CLI command to execute.



#### NOTE

The access level (corresponding to the user name) selected must support the given command.



#### NOTE

Any output from the command will be returned to the workstation submitting the command. Commands that start interactive dialogs (such as **trace**) cannot be used.

### Section 2.5.4

## Executing Secure Commands Remotely via SSH

The remote Secure Shell (SSH) facility can be used from a workstation to cause the product to act upon commands as if they were entered at the CLI prompt. The syntax of the SSH command is usually of the form:

```
ssh auth@ipaddr command_string ; command_string
```

Where:

- *auth* is the user name (i.e. guest, operator or admin).
- *ipaddr* is the address or resolved name of the device.
- *command\_string* is the RUGGEDCOM ROS CLI command (or commands if separated by a ;) to execute.



#### NOTE

The access level (corresponding to the user name) selected must support the given command.

**NOTE**

Any output from the command will be returned to the workstation submitting the command. Commands that start interactive dialogs (such as `trace`) cannot be used.

## Section 2.5.5

## Using SQL Commands

RUGGEDCOM ROS provides an *SQL-like* command facility that allows expert users to perform several operations not possible under the traditional Web or CLI interface. For instance:

- Restoring the contents of a specific table, but not the whole configuration, to their factory defaults.
- Search tables in the database for specific configurations.
- Make changes to tables predicated upon existing configurations.

When combined with RSH, SQL commands provide a means to query and configure large numbers of devices from a central location.

**NOTE**

For a list of parameters available under the `sql` command, refer to [Section 2.5.1, "Available CLI Commands"](#).

**NOTE**

Read/write access to tables containing passwords or shared secrets is unavailable using SQL commands.

**CONTENTS**

- [Section 2.5.5.1, "Finding the Correct Table"](#)
- [Section 2.5.5.2, "Retrieving Information"](#)
- [Section 2.5.5.3, "Changing Values in a Table"](#)
- [Section 2.5.5.4, "Resetting a Table"](#)
- [Section 2.5.5.5, "Using RSH and SQL"](#)

## Section 2.5.5.1

### Finding the Correct Table

Many SQL commands operate upon specific tables in the database, and require the table name to be specified. Navigating the menu system in the console interface to the desired menu and pressing **Ctrl-Z** displays the name of the table. The menu name and the corresponding database table name will be cited.

Another way to find a table name is to type the following in the CLI:

```
sql info tables
```

This command also displays menu names and their corresponding database table names depending upon the features supported by the device. For example:

```
Table Description  
-----
```

```
alarms Alarms
cpuDiags CPU Diagnostics
ethPortCfg Port Parameters
ethPortStats Ethernet Statistics
ethPortStatus Port Status
ipCfg IP Services
```

## Section 2.5.5.2

## Retrieving Information

The following describes various methods for retrieving information about tables and parameters.

### » Retrieving Information from a Table

Use the following command to display a summary of the parameters within a table, as well as their values:

```
sql select from table
```

Where:

- *table* is the name of the table

Example:

```
>sql select from ipAddrtable

IP Address      Subnet          IfIndex  IfStats  IfTime  IfName
172.30.146.88   255.255.224.0  1001     17007888 2994    vlan1

1 records selected
```

### » Retrieving Information About a Parameter from a Table

Use the following command to retrieve information about a specific parameter from a table:

**NOTE**

*The parameter name must be the same as it is displayed in the menu system, unless the name contains spaces (e.g. ip address). Spaces must be replaced with underscores (e.g. ip\_address) or the parameter name must be wrapped in double quotes (e.g. "ip address").*

```
sql select parameter from table
```

Where:

- *parameter* is the name of the parameter
- *table* is the name of the table

Example:

```
>sql select "ip address" from ipSwitchIfCfg

IP Address
192.168.0.1

1 records selected
```

## » Retrieving Information from a Table Using the *Where* Clause

Use the following command to display specific parameters from a table that have a specific value:

```
sql select from table where parameter = value
```

Where:

- *table* is the name of the table
- *parameter* is the name of the parameter
- *value* is the value of the parameter

Example:

```
>sql select from ethportcfg where media = 1000T
```

Port Name	ifName	Media	State	AutoN	Speed	Dupx	FlowCtrl	LFI	Alarm
1 Port 1	1	1000T	Enabled On	Auto	Auto	Off	Off	On	
2 Port 2	2	1000T	Enabled On	Auto	Auto	Off	Off	On	
3 Port 3	3	1000T	Enabled On	Auto	Auto	Off	Off	On	
4 Port 4	4	1000T	Enabled On	Auto	Auto	Off	Off	On	

```
4 records selected
```

Further refine the results by using *and* or *or* operators:

```
sql select from table where parameter = value [ { and | or } | parameter | = | value ...]
```

Where:

- *table* is the name of the table
- *parameter* is the name of the parameter
- *value* is the value of the parameter

Example:

```
>sql select from ethportcfg where media = 1000T and State = enabled
```

Port Name	ifName	Media	State	AutoN	Speed	Dupx	FlowCtrl	LFI	Alarm
1 Port 1	1	1000T	Enabled On	Auto	Auto	Off	Off	on	
2 Port 2	2	1000T	Enabled On	Auto	Auto	Off	Off	On	
3 Port 3	3	1000T	Enabled On	Auto	Auto	Off	Off	On	
4 Port 4	4	1000T	Enabled On	Auto	Auto	Off	Off	On	

```
4 records selected
```

### Section 2.5.5.3

## Changing Values in a Table

Use the following command to change the value of parameters in a table:

```
sql update table set parameter = value
```

Where:

- *table* is the name of the table
- *parameter* is the name of the parameter
- *value* is the value of the parameter

Example:



```
>sql update iplcfg set IP_Address_Type = static
1 records updated
```

Conditions can also be included in the command to apply changes only to parameters that meet specific criteria. In the following example, flow control is enabled on ports that are operating in 100 Mbps full-duplex mode with flow control disabled:

```
>sql update ethportcfg set FlowCtrl = Off where ( Media = 100TX and FlowCtrl = On )
2 records updated
```

#### Section 2.5.5.4

### Resetting a Table

Use the following command to reset a table back to its factory defaults:

```
sql default into table
```

Where:

- *table* is the name of the table

#### Section 2.5.5.5

### Using RSH and SQL

The combination of remote shell scripting and SQL commands offers a means to interrogate and maintain a large number of devices. Consistency of configuration across sites may be verified by this method. The following presents a simple example where the devices to interrogate are drawn from the file *Devices*:

```
C:> type Devices
10.0.1.1
10.0.1.2

C:\> for /F %i in (devices) do rsh %i -l admin,admin sql select from ipAddrtable

C:\>rsh 10.0.1.1 -l admin,admin sql select from ipAddrtable

IP Address      Subnet          IfIndex    IfStats    IfTime     IfName
192.168.0.31    255.255.255.0  1001      274409096  2218      vlan1

1 records selected

C:\>rsh 10.0.1.2 -l admin,admin sql select from ipAddrtable
0 records selected
C:\
```

#### Section 2.6

## Selecting Ports in RUGGEDCOM ROS

Many features in ROS can be configured for one or more ports on the device. The following describes how to specify a single port, a range of ports, or all ports.

Select a single port by specifying the port number:

Select a range of ports using a dash (-) between the first port and the last port in the list:

Select multiple ports by defining a comma-separated list:

Use the *All* option to select all ports in the device, or, if available, use the *None* option to select none of the ports.

## Section 2.7

# Managing the Flash File System

This section describes how to manage the file system.

### CONTENTS

- [Section 2.7.1, “Viewing a List of Flash Files”](#)
- [Section 2.7.2, “Viewing Flash File Details”](#)
- [Section 2.7.3, “Defragmenting the Flash File System”](#)

## Section 2.7.1

# Viewing a List of Flash Files

To view a list of files currently stored in Flash memory, do the following:

1. Log in to the device as an admin user and access the CLI shell. For more information about accessing the CLI shell, refer to [Section 2.5, “Using the Command Line Interface”](#).
2. Type **flashfiles**. A list of files currently in Flash memory is displayed, along with their locations and the amount of memory they consume. For example:

```
>flashfiles
-----
Filename                Base                Size
-----
main.bin                 0xFE959AE0         0x002C5493 (2905235)
syslog.txt               0xFE100080         0x001BFF80 (1834880)
.
.
.

Free Space: 19792360
Used Space: 11664720
Fragmented Space: 5830423
-----
```

## Section 2.7.2

## Viewing Flash File Details

To view the details of a file currently stored in Flash memory, do the following:

1. Log in to the device as an admin user and access the CLI shell. For more information about accessing the CLI shell, refer to [Section 2.5, "Using the Command Line Interface"](#).
2. Display information about a file by typing:

```
flashfiles info filename
```

Where:

- *filename* is the name of the file stored in Flash memory

Details, similar to the following, are displayed.

```
>flashfiles info main.bin

Flash file information for main.bin:
Header version   : 4
Platform        : ROS-CF52

File name       : main.bin
Firmware version: v4.2.2.F.0
Build date      : Sep 27 2014 15:50
File length     : 2624659
Board IDs       : 3d
Header CRC      : 73b4
Header CRC Calc : 73b4
Body CRC        : b441
Body CRC Calc   : b441
```

## Section 2.7.3

## Defragmenting the Flash File System

The flash memory is defragmented automatically whenever there is not enough memory available for a binary upgrade. However, fragmentation can occur whenever a new file is uploaded to the unit. Fragmentation causes sectors of available memory to become separated by ones allocated to files. In some cases, the total available memory might be sufficient for a binary upgrade, but that memory may not be available in one contiguous region.

To defragment the flash memory, do the following:

1. Log in to the device as an admin user and access the CLI shell. For more information about accessing the CLI shell, refer to [Section 2.5, "Using the Command Line Interface"](#).
2. Defragment the flash memory by typing:

```
flashfiles defrag
```

## Section 2.8

## Accessing Maintenance Mode

Maintenance mode is used by service technicians to test and configure internal functions of the device, including BIST (Built-In-Self-Test). It should only be accessed for troubleshooting purposes, or to delete sensitive data.

To access maintenance mode, do the following:

1. Log in to the device as an admin user and access the CLI shell. For more information about accessing the CLI shell, refer to [Section 2.5, "Using the Command Line Interface"](#).

2. At the CLI prompt, type:

```
factory
```

3. When prompted, answer yes and enter the password.

4. At the CLI prompt, type:

```
maintenance
```

The device will boot into maintenance mode.



**NOTE**

*Booting into maintenance mode will automatically delete the `ssl.crt`, `ssh.keys` and `config.csv` files.*

5. To view a list of all available options in maintenance mode, type:

```
help
```

# 3 Getting Started

This section describes startup tasks to be performed during the initial commissioning of the device. Tasks include connecting to the device and accessing the RUGGEDCOM ROS Web User Interface/CLI, as well as configuring a basic network.

## CONTENTS

- [Section 3.1, "Connecting to ROS"](#)
- [Section 3.2, "Configuring a Basic Network"](#)

### Section 3.1

## Connecting to ROS

This section describes the various methods for connecting to the device.

## CONTENTS

- [Section 3.1.1, "Default IP Address"](#)
- [Section 3.1.2, "Connecting Directly"](#)
- [Section 3.1.3, "Connecting Remotely"](#)

### Section 3.1.1

## Default IP Address

The default IP address for the device is 192.168.0.1/24.

### Section 3.1.2

## Connecting Directly

RUGGEDCOM ROS can be accessed through a direct console connection for management and troubleshooting purposes. A console connection provides access to the console interface and CLI.

To establish a console connection to the device, do the following:

1. Connect a workstation (either a terminal or computer running terminal emulation software) to the console port on the device. For more information about the console port, refer to the *RS900GPF Installation Guide*.



**NOTE**

*The baud rate for the device is printed on the chassis exterior near the console port.*

2. Configure the workstation as follows:
  - Speed (baud): 57600
  - Data Bits: 8
  - Parity: None
  - Flow Control: Off
  - Terminal ID: VT100
  - Stop Bit: 1
3. Connect to the device. Once the connection is established, the login form appears. For more information about logging in to the device, refer to [Section 2.1, “Logging In”](#).

Section 3.1.3

## Connecting Remotely

RUGGEDCOM ROS can be accessed securely and remotely either through a Web browser, terminal or workstation running terminal emulation software.

### » Using a Web Browser

Web browsers provide a secure connection to the Web interface for RUGGEDCOM ROS using the SSL (Secure Socket Layer) communication method. SSL encrypts traffic exchanged with its clients.

The RUGGEDCOM ROS Web server guarantees that all communications with the client are private. If a client requests access through an insecure HTTP port, the client is automatically rerouted to the secure port. Access to the Web server through SSL will only be granted to clients that provide a valid user name and password.

To establish a connection through a Web browser, do the following:

1. On the workstation being used to access the device, configure an Ethernet port to use an IP address falling within the subnet of the device. The default IP address is 192.168.0.1/24.

For example, to configure the device to connect to one of the available Ethernet ports, assign an IP address to the Ethernet port on the workstation in the range of 192.168.0.3 to 192.168.0.254.

2. Open a Web browser. For a list of recommended Web browsers, refer to [“System Requirements”](#).



**IMPORTANT!**

*Upon connecting to the device, some Web browsers may report the Web server's certificate cannot be verified against any known certificates. This is expected behavior, and it is safe to instruct the browser to accept the certificate. Once the certificate is accepted, all communications with the Web server through that browser will be secure.*

3. In the address bar, type the IP address for the port that is connected to the network. For example, to access the device using its factory default IP address, type `https://192.168.0.1` and press **Enter**. Once the connection is established, the login screen for the Web interface appears.

For more information about logging in to the device, refer to [Section 2.1, “Logging In”](#). For more information about the Web interface, refer to [Section 2.3, “Using the Web Interface”](#).

## » Using a Terminal or Terminal Emulation Software

A terminal or computer running terminal emulation software provides access to the console interface for RUGGEDCOM ROS through a Telnet, RSH (Remote Shell) or SSH (Secure Shell) service.



### NOTE

*IP services can be restricted to control access to the device. For more information, refer to [Section 4.10, "Configuring IP Services"](#).*

To establish a connection through a terminal or terminal emulation software, do the following:

1. Select the service (i.e. Telnet, RSH or SSH).
2. Enter the IP address for the port that is connected to the network.
3. Connect to the device. Once the connection is established, the login form appears. For more information about logging in to the device, refer to [Section 2.1, "Logging In"](#).

Section 3.2

## Configuring a Basic Network

To configure a basic network, do the following:

1. Connect a computer to one of the switch ports of the device and configure the computer to be on the same subnet as the port.
2. Configure the computer to use the address of VLAN1 as the default gateway.
3. Connect a second computer to a different switch port of the same device, and configure the computer to be on the same subnet as the port.
4. Configure the second computer to use the address of VLAN1 as the default gateway. The default IP address is 192.168.0.1.
5. Make sure both computers connected to the device can ping one another.





# 4 Device Management

This chapter describes how to configure and manage the device and its components, such as module interfaces, logs and files.

## CONTENTS

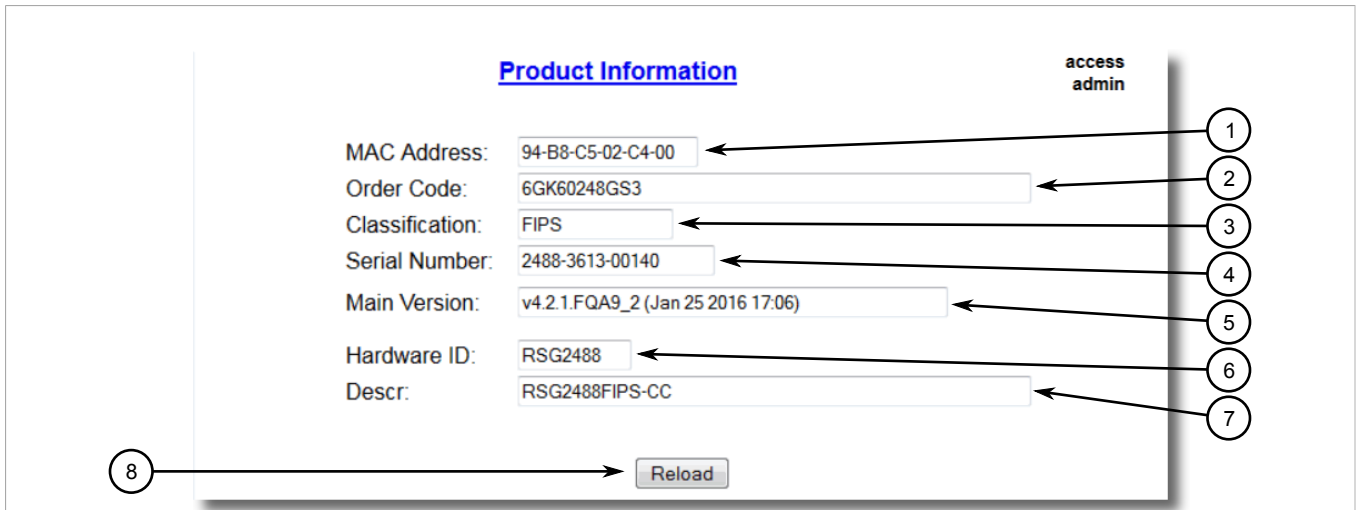
- [Section 4.1, "Viewing Product Information"](#)
- [Section 4.2, "Viewing CPU Diagnostics"](#)
- [Section 4.3, "Restoring Factory Defaults"](#)
- [Section 4.4, "Uploading/Downloading Files"](#)
- [Section 4.5, "Managing Logs"](#)
- [Section 4.6, "Managing Ethernet Ports"](#)
- [Section 4.7, "Managing IP Interfaces"](#)
- [Section 4.8, "Managing IP Gateways"](#)
- [Section 4.9, "Configuring DNS Servers"](#)
- [Section 4.10, "Configuring IP Services"](#)
- [Section 4.11, "Managing Remote Monitoring"](#)
- [Section 4.12, "Upgrading/Downgrading Firmware"](#)
- [Section 4.13, "Resetting the Device"](#)
- [Section 4.14, "Clearing Data"](#)

## Section 4.1

# Viewing Product Information

During troubleshooting or when ordering new devices, Siemens personnel may request specific information about the device, such as the model, order code or serial number.

To view information about the device, navigate to **Diagnostics » View Product Information**. The **Product Information** form appears.



**Figure 8: Product Information Form (Example)**

1. MAC Address Box 2. Order Code Box 3. Classification Box 4. Serial Number Box 5. Main Version Box 6. Hardware ID Box 7. Descr Box 8. Reload Button

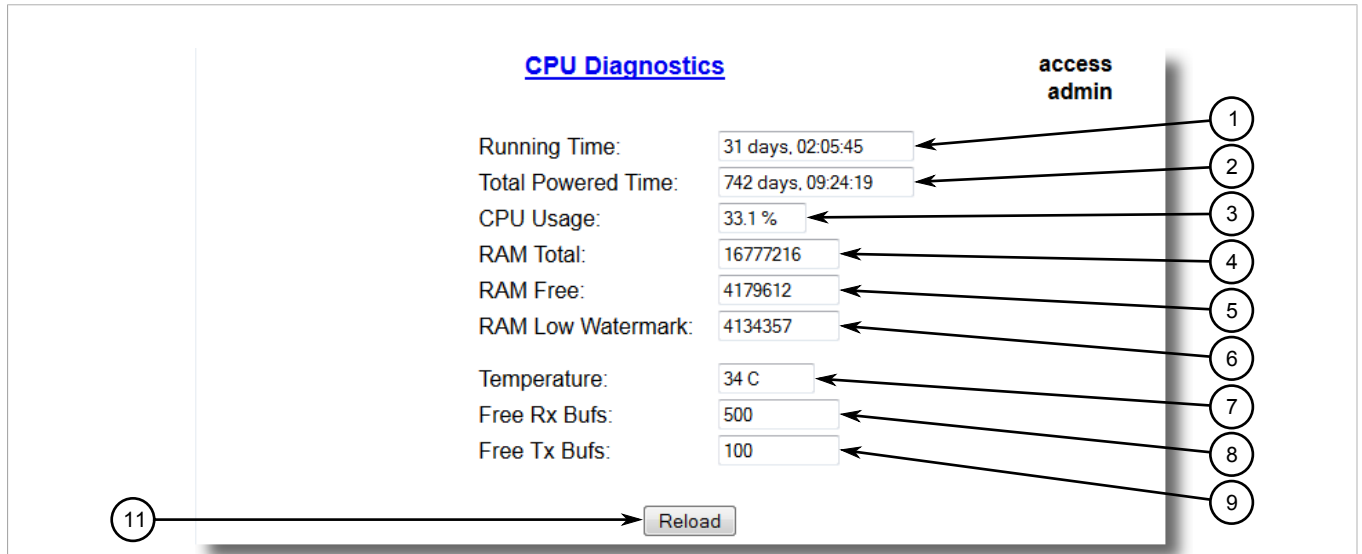
This screen displays the following information:

Parameter	Description
MAC Address	<b>Synopsis:</b> ##-##-##-##-##-## where ## ranges 0 to FF Shows the unique MAC address of the device.
Order Code	<b>Synopsis:</b> Any 57 characters Shows the order code of the device.
Classification	<b>Synopsis:</b> Any 14 characters Provides system classification.  The value <i>Controlled</i> indicates the main firmware is a Controlled release. The value <i>Non-Controlled</i> indicates the main firmware is a Non-Controlled release. The <i>Controlled</i> main firmware can run on Controlled units, but it can not run on Non-Controlled units. The <i>Non-Controlled</i> main firmware can run on both Controlled and Non-Controlled units. The FIPS main firmware is a special <i>Controlled</i> version conforming to FIPS security standards
Serial Number	<b>Synopsis:</b> Any 19 characters Shows the serial number of the device.
Main Version	<b>Synopsis:</b> Any 47 characters Shows the version and build date of the main operating system software.
Hardware ID	<b>Synopsis:</b> { RSG2488, RSG2488v2, RSG2488v3, RMC8388A, RMC8388B, RMC8388C, RSG920P } Shows the type, part number, and revision level of the hardware.
Descr	<b>Synopsis:</b> Any 57 characters

Section 4.2

# Viewing CPU Diagnostics

To view CPU diagnostic information useful for troubleshooting hardware and software performance, navigate to **Diagnostics » View CPU Diagnostics**. The **CPU Diagnostics** form appears.



**Figure 9: CPU Diagnostics Form**

- 1. Running Time Box   2. Total Powered Time Box   3. CPU Usage Box   4. RAM Total Box   5. RAM Free Box   6. RAM Low Watermark Box
- 7. Temperature Box   8. Free Rx Bufs Box   9. Free Tx Bufs Box   10. Reload Button

This screen displays the following information:

Parameter	Description
Running Time	<b>Synopsis:</b> DDDD days, HH:MM:SS The amount of time since the device was last powered on.
Total Powered time	<b>Synopsis:</b> DDDD days, HH:MM:SS The cumulative powered up time of the device.
CPU Usage	<b>Synopsis:</b> 0.0 to 100.0% The percentage of available CPU cycles used for device operation as measured over the last second.
RAM Total	<b>Synopsis:</b> 0 to 4294967295 The total size of RAM in the system.
RAM Free	<b>Synopsis:</b> 0 to 4294967295 The total size of RAM still available.
RAM Low Watermark	<b>Synopsis:</b> 0 to 4294967295 The size of RAM that have never been used during the system runtime.
Temperature	<b>Synopsis:</b> -32768 to 32767 C The temperature on CPU board.
Free Rx Bufs	<b>Synopsis:</b> 0 to 4294967295

Parameter	Description
Free Tx Bufs	Free Rx Buffers. <b>Synopsis:</b> 0 to 4294967295 Free Tx Buffers.

Section 4.3

## Restoring Factory Defaults

The device can be completely or partially restored to its original factory default settings. Excluding groups of parameters from the factory reset, such as those that affect basic connectivity and SNMP management, is useful when communication with the device is still required during the reset.

The following categories are not affected by a selective configuration reset:

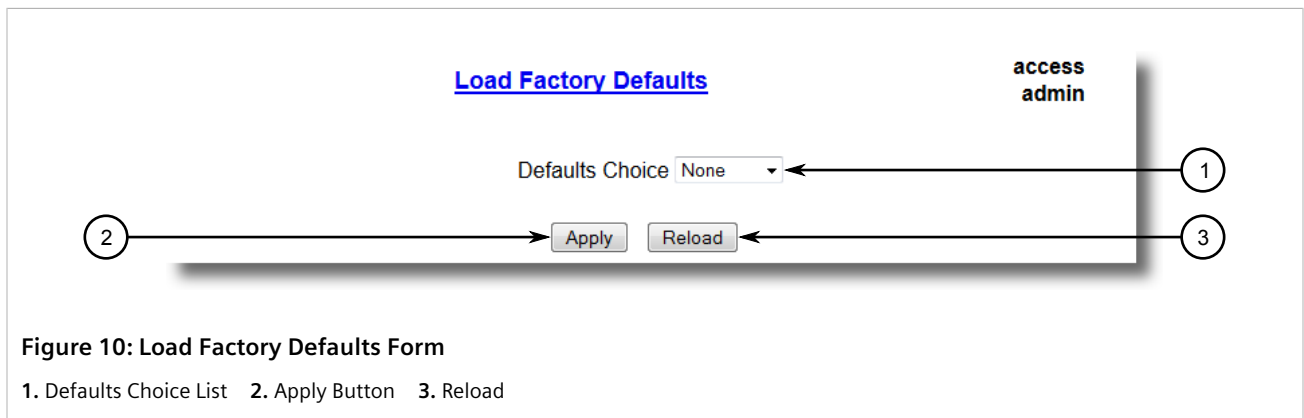
- IP Interfaces
- IP Gateways
- SNMP Users
- SNMP Security to Group Maps
- SNMP Access

In addition, the following categories are not affected by a full or selective configuration reset:

- Time Zone
- DST Offset
- DST Rule

To restore factory defaults, do the following:

1. Navigate to **Diagnostics » Load Factory Defaults**. The **Load Factory Defaults** form appears.



2. Configure the following parameter(s) as required:

**NOTE**  
If the VLAN ID for the Management IP interface is not 1, setting **Defaults Choice** to **Selected** will automatically set it to 1.

Parameter	Description
Defaults Choice	<p><b>Synopsis:</b> { None, Selected, All }</p> <p>Setting some records like IP Interfaces management interface, default gateway, SNMP settings to default value would cause switch not to be accessible with management applications. This parameter allows user to choose to load defaults to Selected tables, which would preserve configuration for tables that are critical for switch management applications, or to force All tables to default settings.</p>

- Click **Apply**.

## Section 4.4

## Uploading/Downloading Files

Files can be transferred between the device and a host computer using any of the following methods:

- Xmodem using the CLI shell over a Telnet or RS-232 console session
- TFTP client using the CLI shell in a console session and a remote TFTP server
- TFTP server from a remote TFTP client
- SFTP (secure FTP over SSH) from a remote SFTP client



### IMPORTANT!

*Telnet and TFTP are disabled by default in RUGGEDCOM ROS. To meet varied customer needs, these protocols can be enabled, but enabling them will break compliance with FIPS 140-2. For more information, refer to the **FIPS 140-2 Non-Proprietary Security Policy** or contact Siemens Customer Support.*



### IMPORTANT!

*Scripts can be used to automate the management of files on the device. However, depending on the size of the target file(s), a delay between any concurrent write and read commands may be required, as the file may not have been fully saved before the read command is issued. A general delay of five seconds is recommended, but testing is encouraged to optimize the delay for the target file(s) and operating environment.*



### NOTE

*The contents of the internal file system are fixed. New files and directories cannot be created, and existing files cannot be deleted. Only the files that can be uploaded to the device can be overwritten.*

Files that may need to be uploaded or downloaded include:

- `main.bin` – the main RUGGEDCOM ROS application firmware image
- `fpga.xsvf` – the FPGA firmware binary image
- `config.csv` – the complete configuration database, in the form of a comma-delimited ASCII text file. This file is only available to admin users.
- `factory.txt` – contains the MAC address, order code and serial number. Factory data must be signed.



### NOTE

*FIPS-compliant versions of RUGGEDCOM ROS only support FIPS-compliant product code.*

- `banner.txt` – contains text that appears on the login screen

#### CONTENTS

- [Section 4.4.1, “Uploading/Downloading Files Using XMODEM”](#)
- [Section 4.4.2, “Uploading/Downloading Files Using a TFTP Client”](#)
- [Section 4.4.3, “Uploading/Downloading Files Using a TFTP Server”](#)
- [Section 4.4.4, “Uploading/Downloading Files Using an SFTP Server”](#)

#### Section 4.4.1

## Uploading/Downloading Files Using XMODEM

To upload or download a file using XMODEM, do the following:



#### NOTE

*This method requires a host computer that has terminal emulation or Telnet software installed and the ability to perform XMODEM transfers.*

1. Establish a connection between the device and the host computer. For more information, refer to [Section 3.1, “Connecting to ROS”](#).
2. Log in to the device as an admin user and access the CLI shell. For more information about accessing the CLI shell, refer to [Section 2.5, “Using the Command Line Interface”](#).
3. At the CLI prompt, type:

```
xmodem [ send | receive ] filename
```

Where:

- `send` sends the file to the host computer
- `receive` pulls the file from the host computer
- `filename` is the name of the file (i.e. `main.bin`)



#### NOTE

*If available in the terminal emulation or Telnet software, select the **XModem 1K** protocol for transmission over the standard **XModem** option.*

4. When the device responds with `Press Ctrl-X to cancel`, launch the XMODEM transfer from the host computer. The device will indicate when the transfer is complete.

The following is an example from the CLI shell of a successful XMODEM file transfer:

```
>xmodem receive main.bin  
Press Ctrl-X to cancel  
Receiving data now ...C  
Received 1428480 bytes. Closing file main.bin ...  
main.bin transferred successfully
```

5. If the file has been uploaded, reset the device. For more information, refer to [Section 4.13, “Resetting the Device”](#)

## Section 4.4.2

## Uploading/Downloading Files Using a TFTP Client

To upload or download a file using a TFTP client, do the following:

**IMPORTANT!**

*TFTP does not define an authentication scheme. Any use of the TFTP client or server is considered highly insecure.*

**NOTE**

*This method requires a TFTP server that is accessible over the network.*

1. Identify the IP address of the computer running the TFTP server.
2. Establish a connection between the device and the host computer. For more information, refer to [Section 3.1, "Connecting to ROS"](#).
3. Log in to the device as an admin user and access the CLI shell. For more information about accessing the CLI shell, refer to [Section 2.5, "Using the Command Line Interface"](#).
4. At the CLI prompt, type:

```
tftp address [ get | put ] source-filename destination-filename
```

Where:

- `get` copies files from the host computer to the device
- `put` copies files from the device to the host computer
- `address` is the IP address of the computer running the TFTP server
- `source-filename` is the name of the file to be transferred
- `destination-filename` is the name of the file (on the device or the TFTP server) that will be replaced during the transfer

The following is an example of a successful TFTP client file transfer:

```
>tftp 10.0.0.1 get ROS-CF52_Main_v4.2.2.F.0.bin main.bin  
TFTP CMD: main.bin transfer ok. Please wait, closing file ...  
TFTP CMD: main.bin loading successful.
```

5. If the file has been uploaded, reset the device. For more information, refer to [Section 4.13, "Resetting the Device"](#)

## Section 4.4.3

## Uploading/Downloading Files Using a TFTP Server

To upload or download a file using a TFTP server, do the following:

**IMPORTANT!**

*TFTP does not define an authentication scheme. Any use of the TFTP client or server is considered highly insecure.*



**NOTE**

*This method requires a host computer that has TFTP server software installed.*



**IMPORTANT!**

*Interaction with TFTP servers is strictly controlled within the device to prevent unauthorized access. Make sure the device is configured to accept the TFTP connection. For more information, refer to [Section 4.10, "Configuring IP Services"](#).*

1. Establish a connection between the device and the host computer. For more information, refer to [Section 3.1, "Connecting to ROS"](#).
2. Initialize the TFTP server on the host computer and launch the TFTP transfer. The server will indicate when the transfer is complete.

The following is an example of a successful TFTP server exchange:

```
C:\>tftp -i 10.1.0.1 put C:\files\ROS-CF52_Main_v4.2.2.F.0.bin main.bin
Transfer successful: 1428480 bytes in 4 seconds, 375617 bytes/s
```

3. If the file has been uploaded, reset the device. For more information, refer to [Section 4.13, "Resetting the Device"](#)

Section 4.4.4

## Uploading/Downloading Files Using an SFTP Server

SFTP (Secure File Transfer Protocol) is a file transfer mechanism that uses SSH to encrypt every aspect of file transfer between a networked client and server.



**NOTE**

*The device does not have an SFTP client and, therefore, can only receive SFTP files from an external source. SFTP requires authentication for the file transfer.*

To upload or download a file using an SFTP server, do the following:



**NOTE**

*This method requires a host computer that has SFTP client software installed.*

1. Establish an SFTP connection between the device and the host computer.
2. Launch the SFTP transfer. The client will indicate when the transfer is complete.

The following is an example of a successful SFTP server exchange:

```
user@host$ sftp admin@ros_ip
Connecting to ros_ip...
admin@ros_ip's password:
sftp> put ROS-CF52_Main_v4.2.2.F.0.bin main.bin
Uploading ROS-CF52_Main_v4.2.2.F.0.bin to /main.bin
ROS-CF52_Main_v4.2.2.F.0.bin 100% 2139KB 48.6KB/s 00:44
sftp> put ROS-MPC83_Main_v4.2.2.F.0.bin main.bin
Uploading ROS-MPC83_Main_v4.2.2.F.0.bin to /main.bin
ROS-MPC83_Main_v4.2.2.F.0.bin 100% 2139KB 48.6KB/s 00:44
sftp>
```



3. If the file has been uploaded, reset the device. For more information, refer to [Section 4.13, “Resetting the Device”](#)

## Section 4.5

## Managing Logs

The crash (`crashlog.txt`) and system (`syslog.txt`) log files contain historical information about events that have occurred during the operation of the device.

The crash log contains debugging information related to problems that might have resulted in unplanned restarts of the device or which may effect the operation of the device. A file size of 0 bytes indicates that no unexpected events have occurred.

The system log contains a record of significant events including startups, configuration changes, firmware upgrades and database re-initializations due to feature additions. The system log will accumulate information until it is full, holding approximately 2 MB of data.

### CONTENTS

- [Section 4.5.1, “Viewing Local and System Logs”](#)
- [Section 4.5.2, “Clearing Local and System Logs”](#)
- [Section 4.5.3, “Configuring the Local System Log”](#)
- [Section 4.5.4, “Managing Remote Logging”](#)
- [Section 4.5.5, “Transferring Secure Audit Logs”](#)

## Section 4.5.1

### Viewing Local and System Logs

The local crash and system logs can both be downloaded from the device and viewed in a text editor. For more information about downloading log files, refer to [Section 4.4, “Uploading/Downloading Files”](#).

To view the system log through the Web interface, navigate to **Diagnostics » View System Log**. The `syslog.txt` form appears.

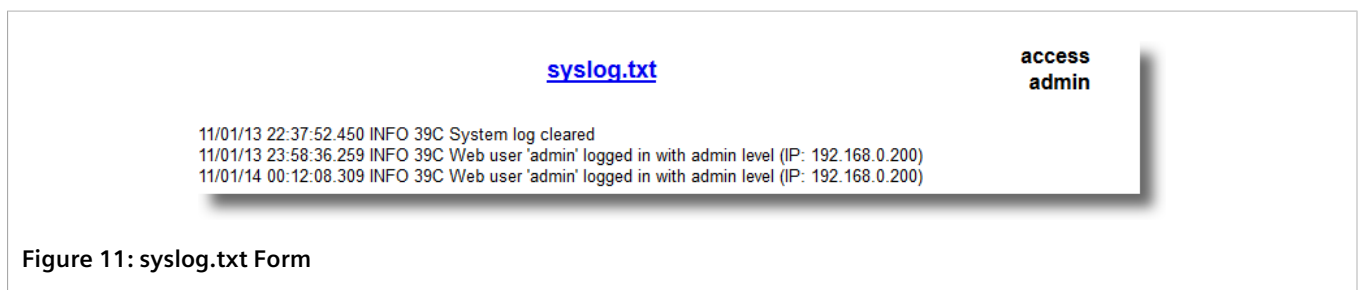


Figure 11: syslog.txt Form

## Section 4.5.2

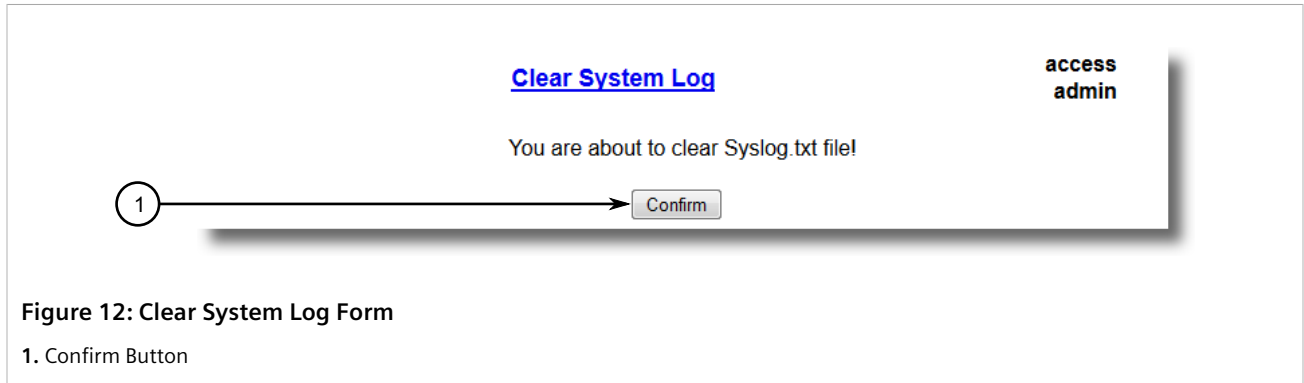
### Clearing Local and System Logs

To clear both the local crash and system logs, log in to the CLI shell as an admin user and type:

**clearlogs**

To clear only the local system log, log in to the Web interface and do the following:

1. Log in to the device as an admin user. For more information, refer to [Section 2.1, “Logging In”](#).
2. Navigate to **Diagnostics » Clear System Log**. The **Clear System Log** form appears.



**Figure 12: Clear System Log Form**

1. Confirm Button

3. Click **Confirm**.

Section 4.5.3

## Configuring the Local System Log

To configure the severity level for the local system log, do the following:



**NOTE**

For maximum reliability, use remote logging. For more information, refer to [Section 4.5.4, “Managing Remote Logging”](#).

1. Navigate to **Administration » Configure Syslog » Configure Local Syslog**. The **Local Syslog** form appears.



**Figure 13: Local Syslog Form**

1. Local Syslog Level
2. Apply Button
3. Reload Button

2. Configure the following parameter(s) as required:

Parameter	Description
Local Syslog Level	<p><b>Synopsis:</b> { EMERGENCY, ALERT, CRITICAL, ERROR, WARNING, NOTICE, INFORMATIONAL, DEBUGGING }</p> <p><b>Default:</b> INFORMATIONAL</p> <p>The severity of the message that has been generated. Note that the severity level selected is considered the minimum severity level for the system. For example, if ERROR</p>

Parameter	Description
	is selected, the system sends any syslog messages generated by Error, Critical, Alert and Emergency.

- Click **Apply**.

Section 4.5.4

## Managing Remote Logging

In addition to the local system log maintained on the device, a remote system log can be configured as well to collect important event messages. The syslog client resides on the device and supports up to 5 collectors (or syslog servers).

The remote syslog protocol, defined in RFC 3164, is a UDP/IP-based transport that enables the device to send event notification messages across IP networks to event message collectors, also known as syslog servers. The protocol is designed to simply transport these event messages from the generating device to the collector(s).



**IMPORTANT!**

*Remote Syslog is disabled by default in RUGGEDCOM ROS. To meet varied customer needs, this protocol can be enabled, but enabling it will break compliance with FIPS 140-2. For more information, refer to the **FIPS 140-2 Non-Proprietary Security Policy** or contact Siemens Customer Support.*

**CONTENTS**

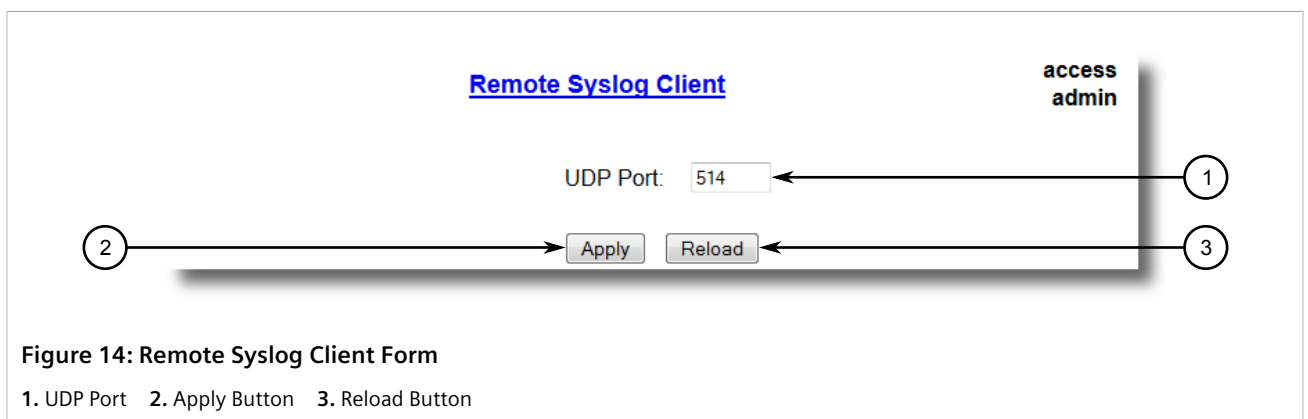
- [Section 4.5.4.1, "Configuring the Remote Syslog Client"](#)
- [Section 4.5.4.2, "Viewing a List of Remote Syslog Servers"](#)
- [Section 4.5.4.3, "Adding a Remote Syslog Server"](#)
- [Section 4.5.4.4, "Deleting a Remote Syslog Server"](#)

Section 4.5.4.1

### Configuring the Remote Syslog Client

To configure the remote syslog client, do the following:

- Navigate to **Administration » Configure Syslog » Configure Remote Syslog Client**. The **Remote Syslog Client** form appears.



**Figure 14: Remote Syslog Client Form**

1. UDP Port 2. Apply Button 3. Reload Button

- Configure the following parameter(s) as required:

Parameter	Description
UDP Port	<p><b>Synopsis:</b> 1025 to 65535 or { 514 }</p> <p><b>Default:</b> 514</p> <p>The local UDP port through which the client sends information to the server(s).</p>

- Click **Apply**.

#### Section 4.5.4.2

### Viewing a List of Remote Syslog Servers

To view a list of known remote syslog servers, navigate to **Administration » Configure Syslog » Configure Remote Syslog Server**. The **Remote Syslog Server** table appears.

The screenshot shows a web interface for configuring remote syslog servers. At the top, there is a title "Remote Syslog Server" and a user name "access admin". Below the title is a link "InsertRecord". In the center, there is a table with the following data:

IP Address	UDP Port	Facility	Severity
<a href="#">192.168.0.1</a>	514	LOCAL7	DEBUGGING
<a href="#">192.168.3.1</a>	514	USER	WARNING

Figure 15: Remote Syslog Server Table

If remote syslog servers have not been configured, add the servers as needed. For more information, refer to [Section 4.5.4.3, "Adding a Remote Syslog Server"](#).

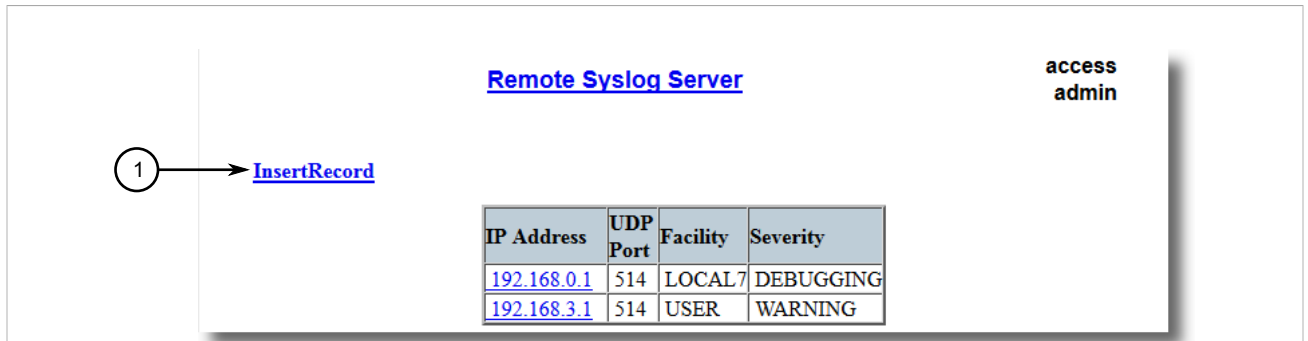
#### Section 4.5.4.3

### Adding a Remote Syslog Server

RUGGEDCOM ROS supports up to 5 remote syslog servers (or collectors). Similar to the local system log, a remote system log server can be configured to log information at a specific severity level. Only messages of a severity level equal to or greater than the specified severity level are written to the log.

To add a remote syslog server to the list of known servers, do the following:

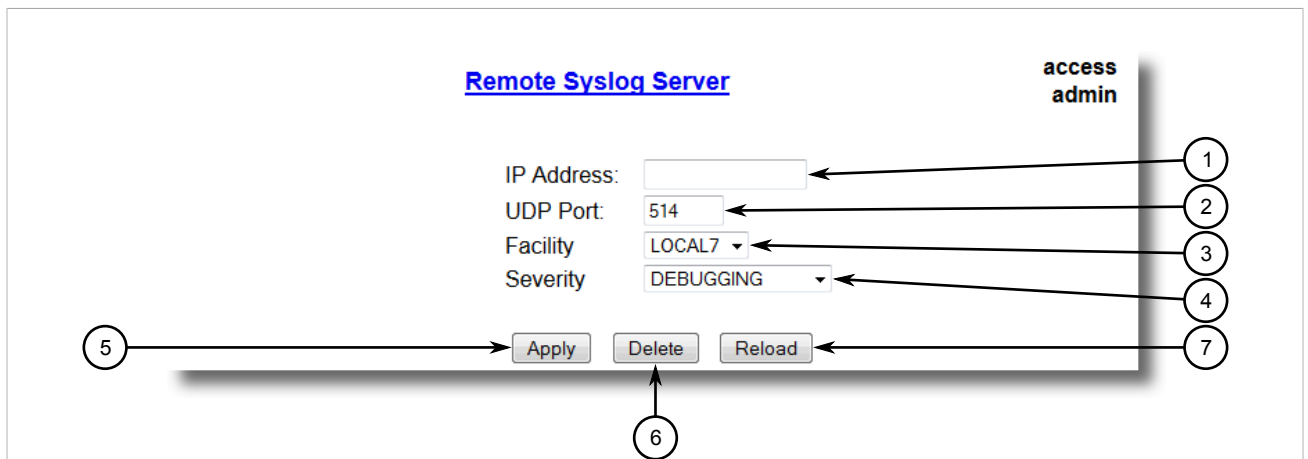
- Navigate to **Administration » Configure Syslog » Configure Remote Syslog Server**. The **Remote Syslog Server** table appears.



**Figure 16: Remote Syslog Server Table**

1. InsertRecord

2. Click **InsertRecord**. The **Remote Syslog Server** form appears.



**Figure 17: Remote Syslog Server Form**

1. IP Address Box 2. UDP Port Box 3. Facility Box 4. Severity Box 5. Apply Button 6. Delete Button 7. Reload Button

3. Configure the following parameter(s) as required:

Parameter	Description
IP Address	<b>Synopsis:</b> ###.###.###.### where ### ranges from 0 to 255 Syslog server IP Address.
UDP Port	<b>Synopsis:</b> 1025 to 65535 or { 514 } <b>Default:</b> 514 The UDP port number on which the remote server listens.
Facility	<b>Synopsis:</b> { USER, LOCAL0, LOCAL1, LOCAL2, LOCAL3, LOCAL4, LOCAL5, LOCAL6, LOCAL7 } <b>Default:</b> LOCAL7 Syslog Facility is one information field associated with a syslog message. The syslog facility is the application or operating system component that generates a log message. ROS map all syslog logging information onto a single facility which is configurable by user to facilitate remote syslog server.

Parameter	Description
Severity	<p><b>Synopsis:</b> { EMERGENCY, ALERT, CRITICAL, ERROR, WARNING, NOTICE, INFORMATIONAL, DEBUGGING }</p> <p><b>Default:</b> DEBUGGING</p> <p>The severity level is the severity of the message that has been generated. Please note that the severity level user select is accepted as the minimum severity level for the system. For example, if user selects the severity level as 'Error' then the system send any syslog message originated by Error, Critical, Alert and Emergency.</p>

- Click **Apply**.

Section 4.5.4.4

## Deleting a Remote Syslog Server

To delete a remote syslog server from the list of known servers, do the following:

- Navigate to **Administration » Configure Syslog » Configure Remote Syslog Server**. The **Remote Syslog Server** table appears.

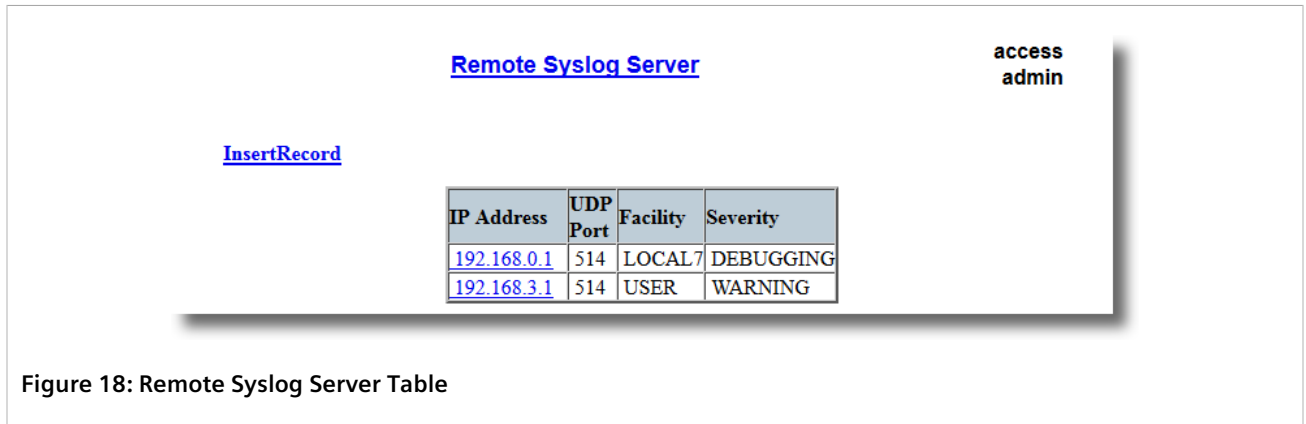


Figure 18: Remote Syslog Server Table

- Select the server from the table. The **Remote Syslog Server** form appears.

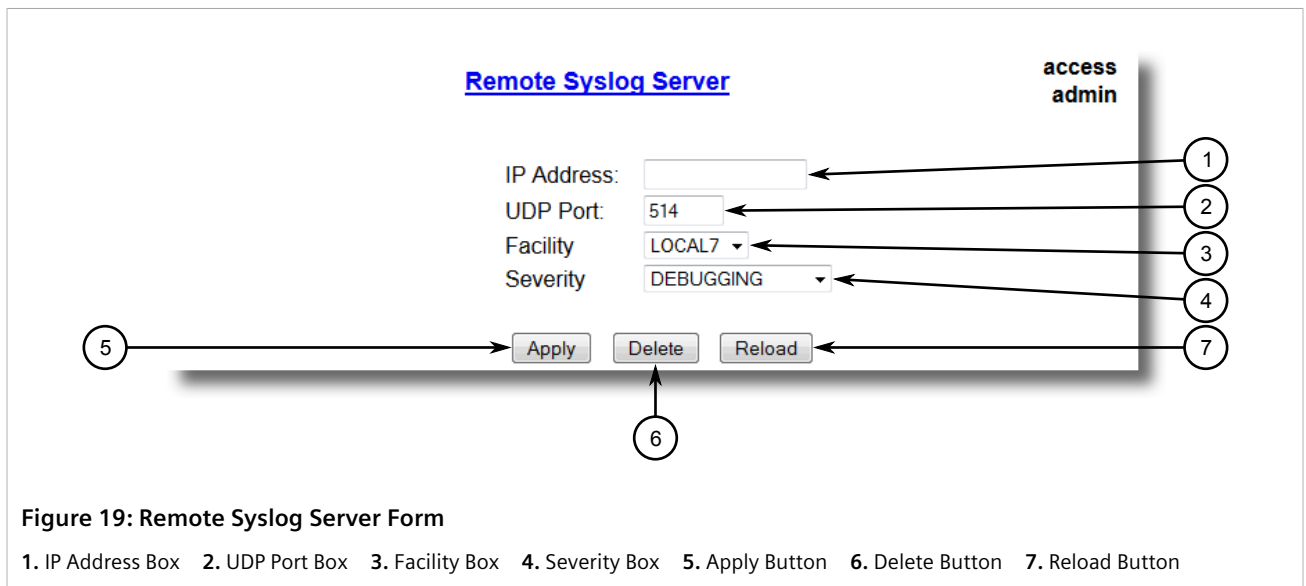


Figure 19: Remote Syslog Server Form

1. IP Address Box   2. UDP Port Box   3. Facility Box   4. Severity Box   5. Apply Button   6. Delete Button   7. Reload Button

3. Click **Delete**.

## Section 4.5.5

## Transferring Secure Audit Logs

RUGGEDCOM ROS can facilitate the display of real-time log entries locally to a PC, and if desired forward encrypted logs to one or more remote servers.

Detailed instructions for transferring secure audit logs are described in the Siemens FAQ: *How to Transfer Secure Audit Logs*, available from <https://www.siemens.com/ruggedcom>.

A required utility is available from Siemens to extract the logs, encrypt them and transfer them to a remote server. For more information, contact Siemens Customer Support.

## Section 4.6

## Managing Ethernet Ports

This section describes how to manage Ethernet ports.

**NOTE**

*For information about configuring remote monitoring for Ethernet ports, refer to [Section 4.11](#), "Managing Remote Monitoring".*

**CONTENTS**

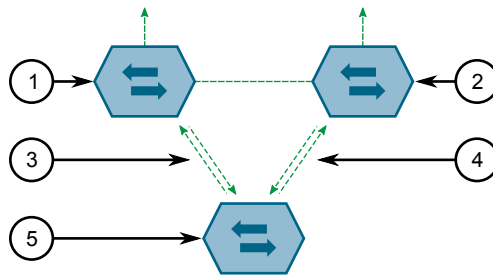
- [Section 4.6.1, "Controller Protection Through Link Fault Indication \(LFI\)"](#)
- [Section 4.6.2, "Viewing the Status of Ethernet Ports"](#)
- [Section 4.6.3, "Viewing Statistics for All Ethernet Ports"](#)
- [Section 4.6.4, "Viewing Statistics for Specific Ethernet Ports"](#)
- [Section 4.6.5, "Clearing Statistics for Specific Ethernet Ports"](#)
- [Section 4.6.6, "Configuring an Ethernet Port"](#)
- [Section 4.6.7, "Configuring Port Rate Limiting"](#)
- [Section 4.6.8, "Configuring Port Mirroring"](#)
- [Section 4.6.9, "Configuring Link Detection"](#)
- [Section 4.6.10, "Managing SFP Transceivers"](#)
- [Section 4.6.11, "Managing PoE Ports "](#)
- [Section 4.6.12, "Detecting Cable Faults"](#)
- [Section 4.6.13, "Resetting Ethernet Ports"](#)

Section 4.6.1

# Controller Protection Through Link Fault Indication (LFI)

Modern industrial controllers often feature backup Ethernet ports used in the event of a link failure. When these interfaces are supported by media (such as fiber) that employ separate transmit and receive paths, the interface can be vulnerable to failures that occur in only one of the two paths.

Consider for instance two switches (A and B) connected to a controller. Switch A is connected to the main port on the controller, while Switch B is connected to the backup port, which is shut down by the controller while the link with Switch A is active. Switch B must forward frames to the controller through Switch A.



**Figure 20: Example**

1. Switch A 2. Switch B 3. Main Transmit Path 4. Backup Transmit Path 5. Controller

If the transmit path from the controller to Switch A fails, Switch A still generates a link signal to the controller through the receive path. The controller still detects the link with Switch A and does not failover to the backup port.

This situation illustrates the need for a notification method that tells a link partner when the link integrity signal has stopped. Such a method natively exists in some link media, but not all.

100Base-TX, 1000Base-T, 1000Base-X	Includes a built-in auto-negotiation feature (i.e. a special flag called Remote Fault Indication is set in the transmitted auto-negotiation signal).
100Base-FX Links	Includes a standard Far-End-Fault-Indication (FEFI) feature defined by the IEEE 802.3 standard for this link type. This feature includes: <ul style="list-style-type: none"> <li>• <b>Transmitting FEFI</b> Transmits a modified link integrity signal in case a link failure is detected (i.e. no link signal is received from the link partner)</li> <li>• <b>Detecting FEFI</b> Indicates link loss in case an FEFI signal is received from the link partner</li> </ul>
10Base-FL Links	No standard support.

10Base-FL links do not have a native link partner notification mechanism and FEFI support in 100Base-FX links is optional according to the IEEE 802.3 standard, which means that some links partners may not support it.

Siemens offers an advanced Link-Fault-Indication (LFI) feature for the links that do not have a native link partner notification mechanism. With LFI enabled, the device bases the generation of a link integrity signal upon its reception of a link signal. In the example described previously, if switch A fails to receive a link signal from the controller, it will stop generating a link signal. The controller will detect the link failure and failover to the backup port.





**IMPORTANT!**

If both link partners have the LFI feature, it **must not** be enabled on both sides of the link. If it is enabled on both sides, the link will never be established, as each link partner will be waiting for the other to transmit a link signal.

The switch can also be configured to flush the MAC address table for the controller port. Frames destined for the controller will be flooded to Switch B where they will be forwarded to the controller (after the controller transmits its first frame).

Section 4.6.2

## Viewing the Status of Ethernet Ports

To view the current status of each Ethernet port, navigate to **Ethernet Ports » View Port Status**. The **Port Status** table appears.

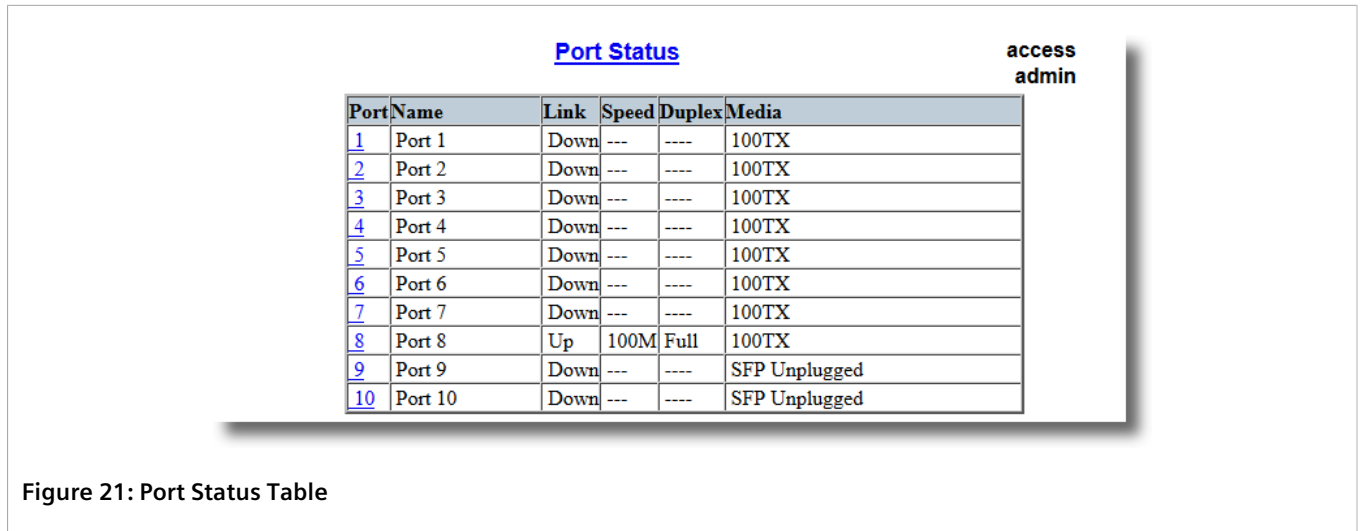


Figure 21: Port Status Table

This table displays the following information:

Parameter	Description
Port	<b>Synopsis:</b> 1 to maximum port number The port number as seen on the front plate silkscreen of the switch.
Name	<b>Synopsis:</b> Any 15 characters A descriptive name that may be used to identify the device connected on that port.
Link	<b>Synopsis:</b> { ----, ---, Down, Up } The port's link status.
Speed	<b>Synopsis:</b> { ---, 10M, 100M, 1G, 10G } The port's current speed.
Duplex	<b>Synopsis:</b> { ----, Half, Full } The port's current duplex status.

Section 4.6.3

## Viewing Statistics for All Ethernet Ports

To view statistics collected for all Ethernet ports, navigate to *Ethernet Stats » View Ethernet Statistics*. The **Ethernet Statistics** table appears.

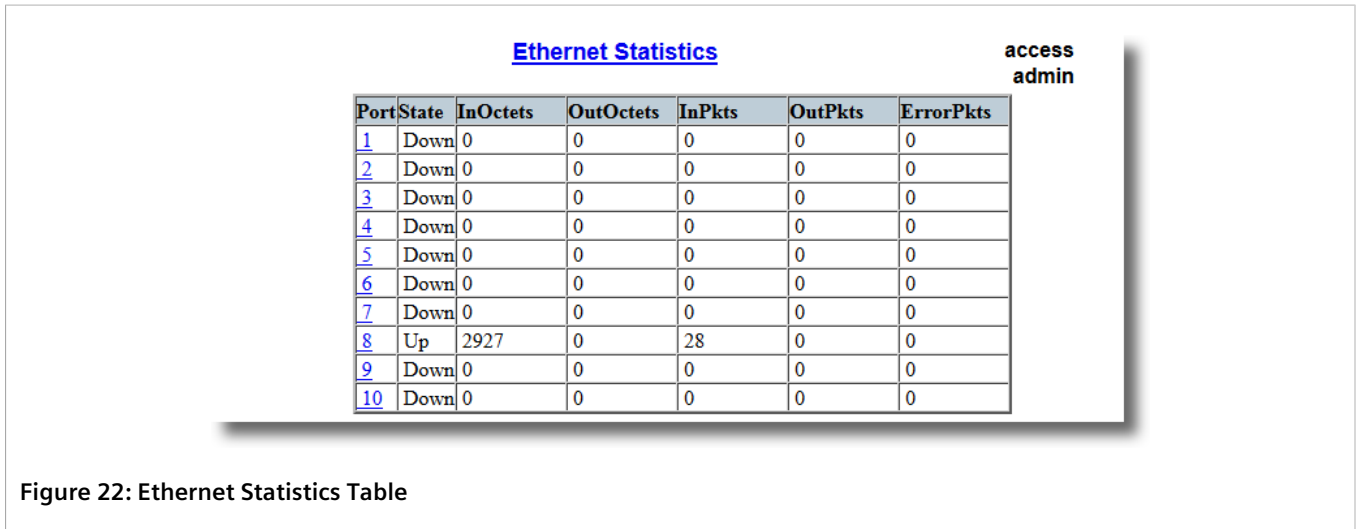


Figure 22: Ethernet Statistics Table

This table displays the following information:

Parameter	Description
Port	<b>Synopsis:</b> 1 to maximum port number The port number as seen on the front plate silkscreen of the switch.
State	<b>Synopsis:</b> { ----, ----, Down, Up }
InOctets	<b>Synopsis:</b> 0 to 4294967295 The number of octets in received good packets (Unicast+Multicast+Broadcast) and dropped packets.
OutOctets	<b>Synopsis:</b> 0 to 4294967295 The number of octets in transmitted good packets.
InPkts	<b>Synopsis:</b> 0 to 4294967295 The number of received good packets (Unicast+Multicast+Broadcast) and dropped packets.
OutPkts	<b>Synopsis:</b> 0 to 4294967295 The number of transmitted good packets.
ErrorPkts	<b>Synopsis:</b> 0 to 4294967295 The number of any type of erroneous packet.

Section 4.6.4

## Viewing Statistics for Specific Ethernet Ports

To view statistics collected for specific Ethernet ports, navigate to *Ethernet Stats » View Ethernet Port Statistics*. The **Ethernet Port Statistics** table appears.

**Ethernet Port Statistics**

**access  
admin**

Port	InOctets	OutOctets	InPkts	OutPkts	TotalInOctets	TotalInPkts
1	2374236	2157956	13627	32698	2374236	13627
2	192516	2399229	2049	33996	192516	2049
3	0	0	0	0	0	0
4	0	0	0	0	0	0
5	0	0	0	0	0	0
6	0	0	0	0	0	0
7	0	0	0	0	0	0
8	10077906	314359	104258	1010	10077906	104258
9	0	0	0	0	0	0
10	0	0	0	0	0	0

**Figure 23: Ethernet Port Statistics Table**

This table displays the following information:

Parameter	Description
Port	<b>Synopsis:</b> 1 to maximum port number The port number as seen on the front plate silkscreen of the switch.
InOctets	<b>Synopsis:</b> 0 to 18446744073709551615 The number of octets in received good packets (Unicast+Multicast+Broadcast) and dropped packets.
OutOctets	<b>Synopsis:</b> 0 to 18446744073709551615 The number of octets in transmitted good packets.
InPkts	<b>Synopsis:</b> 0 to 18446744073709551615 The number of received good packets (Unicast+Multicast+Broadcast) and dropped packets.
OutPkts	<b>Synopsis:</b> 0 to 18446744073709551615 The number of transmitted good packets.
TotalInOctets	<b>Synopsis:</b> 0 to 18446744073709551615 The total number of octets of all received packets. This includes data octets of rejected and local packets which are not forwarded to the switching core for transmission. It should reflect all the data octets received on the line.
TotalInPkts	<b>Synopsis:</b> 0 to 18446744073709551615 The number of received packets. This includes rejected, dropped local, and packets which are not forwarded to the switching core for transmission. It should reflect all packets received on the line.
InBroadcasts	<b>Synopsis:</b> 0 to 18446744073709551615 The number of good Broadcast packets received.
InMulticasts	<b>Synopsis:</b> 0 to 18446744073709551615 The number of good Multicast packets received.
CRCAAlignErrors	<b>Synopsis:</b> 0 to 4294967295 The number of packets received which meet all the following conditions: <ul style="list-style-type: none"> <li>• Packet data length is between 64 and 1536 octets inclusive.</li> <li>• Packet has invalid CRC.</li> <li>• Collision Event has not been detected.</li> </ul>

Parameter	Description
	<ul style="list-style-type: none"> <li>Late Collision Event has not been detected.</li> </ul>
OversizePkts	<p><b>Synopsis:</b> 0 to 4294967295</p> <p>The number of packets received with data length greater than 1536 octets and valid CRC.</p>
Fragments	<p><b>Synopsis:</b> 0 to 4294967295</p> <p>The number of packets received which meet all the following conditions:</p> <ul style="list-style-type: none"> <li>Packet data length is less than 64 octets, or packet without SFD and is less than 64 octets in length.</li> <li>Collision Event has not been detected.</li> <li>Late Collision Event has not been detected.</li> <li>Packet has invalid CRC.</li> </ul>
Jabbers	<p><b>Synopsis:</b> 0 to 4294967295</p> <p>The number of packets which meet all the following conditions:</p> <ul style="list-style-type: none"> <li>Packet data length is greater than 1536 octets.</li> <li>Packet has invalid CRC.</li> </ul>
Collisions	<p><b>Synopsis:</b> 0 to 4294967295</p> <p>The number of received packets for which Collision Event has been detected.</p>
LateCollisions	<p><b>Synopsis:</b> 0 to 4294967295</p> <p>The number of received packets for which Late Collision Event has been detected.</p>
Pkt64Octets	<p><b>Synopsis:</b> 0 to 4294967295</p> <p>The number of received and transmitted packets with size of 64 octets. This includes received and transmitted packets as well as dropped and local received packets. This does not include rejected received packets.</p>
Pkt65to127Octets	<p><b>Synopsis:</b> 0 to 4294967295</p> <p>The number of received and transmitted packets with size of 65 to 127 octets. This includes received and transmitted packets as well as dropped and local received packets. This does not include rejected received packets.</p>
Pkt128to255Octets	<p><b>Synopsis:</b> 0 to 4294967295</p> <p>The number of received and transmitted packets with size of 128 to 257 octets. This includes received and transmitted packets as well as dropped and local received packets. This does not include rejected received packets.</p>
Pkt256to511Octets	<p><b>Synopsis:</b> 0 to 4294967295</p> <p>The number of received and transmitted packets with size of 256 to 511 octets. This includes received and transmitted packets as well as dropped and local received packets. This does not include rejected received packets.</p>
Pkt512to1023Octets	<p><b>Synopsis:</b> 0 to 4294967295</p> <p>The number of received and transmitted packets with size of 512 to 1023 octets. This includes received and transmitted packets as well as dropped and local received packets. This does not include rejected received packets.</p>
Pkt1024to1536Octets	<p><b>Synopsis:</b> 0 to 4294967295</p> <p>The number of received and transmitted packets with size of 1024 to 1536 octets. This includes received and transmitted packets as well as dropped and local received packets. This does not include rejected received packets.</p>
DropEvents	<p><b>Synopsis:</b> 0 to 4294967295</p> <p>The number of received packets that are dropped due to lack of receive buffers.</p>
OutMulticasts	<p><b>Synopsis:</b> 0 to 18446744073709551615</p> <p>The number of transmitted Multicast packets. This does not include Broadcast packets.</p>

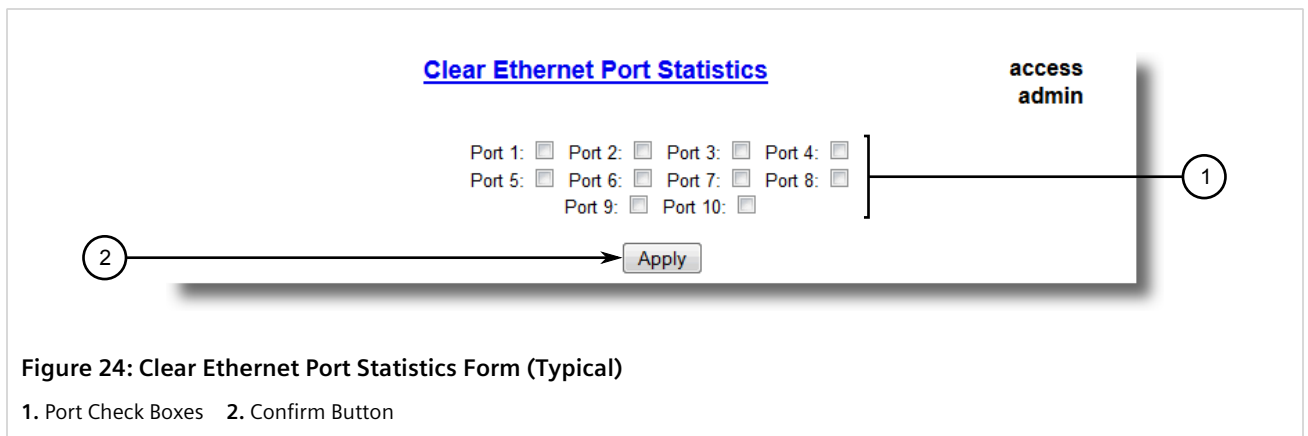
Parameter	Description
OutBroadcasts	<b>Synopsis:</b> 0 to 18446744073709551615 The number of transmitted Broadcast packets.
UndersizePkts	<b>Synopsis:</b> 0 to 4294967295 The number of received packets which meet all the following conditions: <ul style="list-style-type: none"> <li>• Packet data length is less than 64 octets.</li> <li>• Collision Event has not been detected.</li> <li>• Late Collision Event has not been detected.</li> <li>• Packet has valid CRC.</li> </ul>

Section 4.6.5

## Clearing Statistics for Specific Ethernet Ports

To clear the statistics collected for one or more Ethernet ports, do the following:

1. Navigate to **Ethernet Stats » Clear Ethernet Port Statistics**. The **Clear Ethernet Port Statistics** form appears.



**Figure 24: Clear Ethernet Port Statistics Form (Typical)**

1. Port Check Boxes 2. Confirm Button

2. Select one or more Ethernet ports.
3. Click **Confirm**.

Section 4.6.6

## Configuring an Ethernet Port

To configure an Ethernet port, do the following:



**NOTE**

*Depending on the required link media type, an SFP port may require some explicit configuration. Before configuring an SFP port, refer to [Section 4.6.10.1, "SFP Transceiver Requirements"](#).*

1. Navigate to **Ethernet Ports » Configure Port Parameters**. The **Port Parameters** table appears.

**Port Parameters**

**access  
admin**

Port	Name	Media	State	AutoN	Speed	Dupx	FlowCtrl	LFI	Alarm	Act on LinkDown
2	Port 2	100TX	Enabled	On	Auto	Auto	Off	Off	On	Do nothing
4	Port 4	100TX	Enabled	On	Auto	Auto	Off	Off	On	Do nothing

**Figure 25: Port Parameters Table**

- Select an Ethernet port. The **Port Parameters** form appears.

**Port Parameters**

**access  
admin**

Port:  1

Name:  2

Media:  3

State: Disabled:  Enabled:  4

AutoN: On:  Off:  5

Speed:  6

Dupx:  7

FlowCtrl: On:  Off:  8

LFI:  9

Alarm: On:  Off:  10

Act on LinkDown: Do nothing:  Admin Disable:  11



12 13

**Figure 26: Port Parameters Form**

1. Port Box 2. Name Box 3. Media Box 4. State Options 5. AutoN Options 6. Speed List 7. Dupx List 8. FlowCtrl Options  
9. LFI Option 10. Alarm Options 11. Act on LinkDown Options 12. Apply Button 13. Reload Button

- Configure the following parameter(s) as required:

Parameter	Description
Port	<b>Synopsis:</b> 1 to maximum port number <b>Default:</b> 1 The port number as seen on the front plate silkscreen of the switch.
Name	<b>Synopsis:</b> Any 15 characters <b>Default:</b> Port x A descriptive name that may be used to identify the device connected on that port.
Media	<b>Synopsis:</b> { 100TX, 10FL, 100FX, 1000X, 1000T, 802.11g, EoVDSL, 100TX Only, 10FL/100SX, 10GX } <b>Default:</b> 100TX The type of the port media.
State	<b>Synopsis:</b> { Disabled, Enabled }

Parameter	Description
	<p><b>Default:</b> Enabled</p> <p>Disabling a port will prevent all frames from being sent and received on that port. Also, when disabled link integrity signal is not sent so that the link/activity LED will never be lit. You may want to disable a port for troubleshooting or to secure it from unauthorized connections.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;">  <p><b>NOTE</b> <i>Disabling a port whose media type is set to <b>802.11g</b> disables the corresponding wireless module.</i></p> </div>
AutoN	<p><b>Synopsis:</b> { Off, On }</p> <p><b>Default:</b> On</p> <p>Enable or disable IEEE 802.3 auto-negotiation. Enabling auto-negotiation results in speed and duplex being negotiated upon link detection; both end devices must be auto-negotiation compliant for the best possible results. 10Mbps and 100Mbps fiber optic media do not support auto-negotiation so these media must be explicitly configured to either half or full duplex. Full duplex operation requires that both ends are configured as such or else severe frame loss will occur during heavy network traffic.</p>
Speed	<p><b>Synopsis:</b> { Auto, 10M, 100M, 1G }</p> <p><b>Default:</b> Auto</p> <p>Speed (in Megabit-per-second or Gigabit-per-second). If auto-negotiation is enabled, this is the speed capability advertised by the auto-negotiation process. If auto-negotiation is disabled, the port is explicitly forced to this speed mode.</p> <p>AUTO means advertise all supported speed modes.</p>
Dupx	<p><b>Synopsis:</b> { Auto, Half, Full }</p> <p><b>Default:</b> Auto</p> <p>Duplex mode. If auto-negotiation is enabled, this is the duplex capability advertised by the auto-negotiation process. If auto-negotiation is disabled, the port is explicitly forced to this duplex mode.</p> <p>AUTO means advertise all supported duplex modes.</p>
Flow Control	<p><b>Synopsis:</b> { Off, On }</p> <p><b>Default:</b> On</p> <p>Flow Control is useful for preventing frame loss during times of severe network traffic. Examples of this include multiple source ports sending to a single destination port or a higher speed port bursting to a lower speed port.</p> <p>When the port is half-duplex it is accomplished using 'backpressure' where the switch simulates collisions causing the sending device to retry transmissions according to the Ethernet backoff algorithm.</p> <p>When the port is full-duplex it is accomplished using PAUSE frames which causes the sending device to stop transmitting for a certain period of time.</p>
LFI	<p><b>Synopsis:</b> { Off, On }</p> <p><b>Default:</b> Off</p> <p>Enabling Link-Fault-Indication (LFI) inhibits transmitting link integrity signal when the receive link has failed. This allows the device at far end to detect link failure under all circumstances.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;">  <p><b>NOTE</b> <i>This feature must not be enabled at both ends of a fiber link.</i></p> </div>
Alarm	<p><b>Synopsis:</b> { On, Off }</p> <p><b>Default:</b> On</p> <p>Disabling link state alarms will prevent alarms and LinkUp and LinkDown SNMP traps from being sent for that port.</p>



**NOTE**

*If one end of the link is fixed to a specific speed and duplex type and the peer auto-negotiates, there is a strong possibility the link will either fail to raise, or raise with the wrong settings on the auto-negotiating side. The auto-negotiating peer will fall back to half-duplex operation, even when the fixed side is full duplex. Full-duplex operation requires that both ends are configured as such or else severe frame loss will occur during heavy network traffic. At lower traffic volumes the link may display few, if any, errors. As the traffic volume rises, the fixed negotiation side will begin to experience dropped packets, while the auto-negotiating side will experience excessive collisions. Ultimately, as traffic load approaches 100%, the link will become entirely unusable. These problems can be avoided by always configuring ports to the appropriate fixed values.*

4. Click **Apply**.

Section 4.6.7

## Configuring Port Rate Limiting

To configure port rate limiting, do the following:

1. Navigate to **Ethernet Ports » Configure Port Rate Limiting**. The **Port Rate Limiting** table appears.

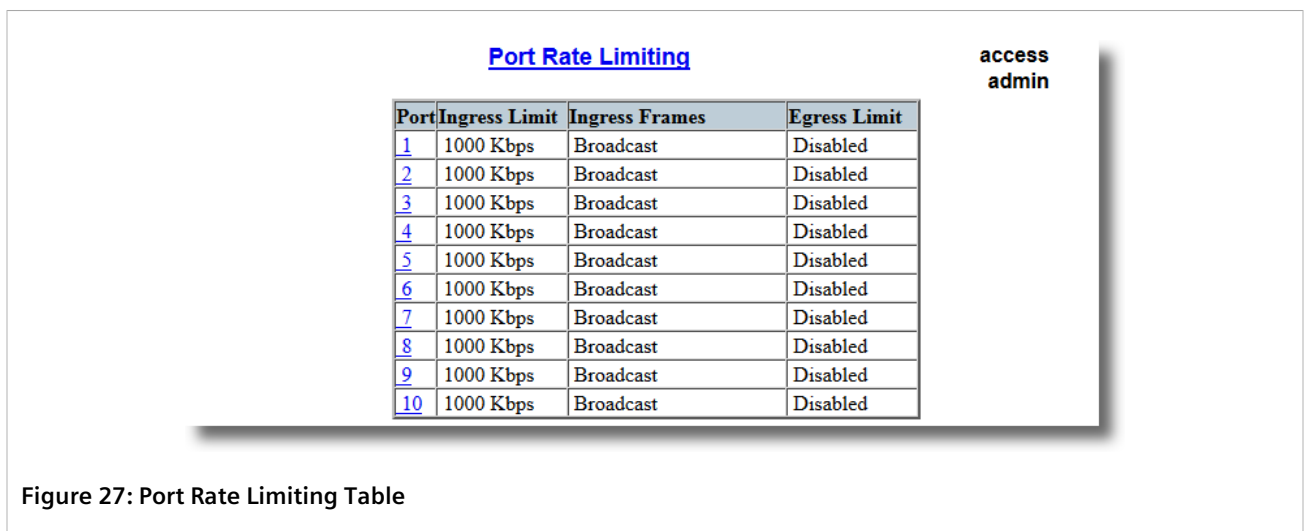
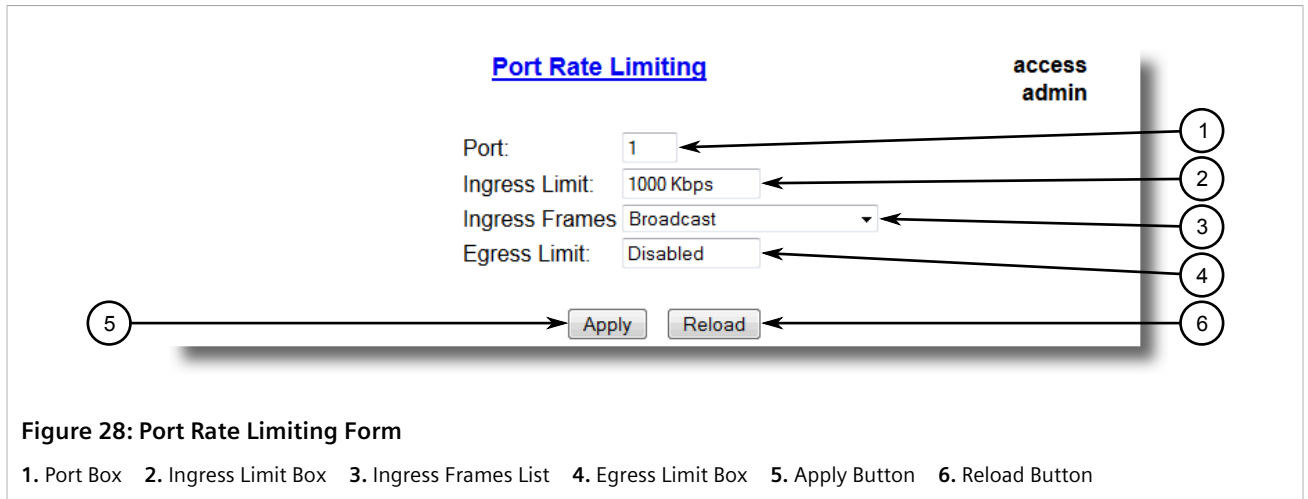


Figure 27: Port Rate Limiting Table

2. Select an Ethernet port. The **Port Rate Limiting** form appears.





**Figure 28: Port Rate Limiting Form**

1. Port Box 2. Ingress Limit Box 3. Ingress Frames List 4. Egress Limit Box 5. Apply Button 6. Reload Button

3. Configure the following parameter(s) as required:

Parameter	Description
Port	<b>Synopsis:</b> 1 to maximum port number <b>Default:</b> 1 The port number as seen on the front plate silkscreen of the switch.
Ingress Limit	<b>Synopsis:</b> 62 to 256000 Kbps or { Disabled } <b>Default:</b> 1000 Kbps The rate after which received frames (of the type described by the ingress frames parameter) will be discarded by the switch.
Ingress Frames	<b>Synopsis:</b> { Broadcast, Bcast&Mcast, Bcast&Mcast&FloodUcast, Bcast&FloodUcast, FloodUcast, All } <b>Default:</b> Broadcast This parameter specifies the types of frames to be rate-limited on this port. It applies only to received frames: <ul style="list-style-type: none"> <li>• Broadcast - only broadcast frames</li> <li>• Bcast&amp;Mcast - broadcast and multicast frames</li> <li>• Bcast&amp;FloodUcast - broadcast and flooded unicast frames</li> <li>• Bcast&amp;Mcast&amp;FloodUcast - broadcast, multicast and flooded unicast frames</li> <li>• FloodUcast - only flooded unicast frames</li> <li>• All - all (multicast, broadcast and unicast) frames</li> </ul>
Egress Limit	<b>Synopsis:</b> { Broadcast, Multicast, Mcast&FloodUcast, All }>62 to 256000 Kbps or { Disabled } <b>Default:</b> Disabled The maximum rate at which the switch will transmit (multicast, broadcast and unicast) frames on this port. The switch will discard frames to meet this rate if required.

4. Click **Apply**.

Section 4.6.8

# Configuring Port Mirroring

Port mirroring is a troubleshooting tool that copies, or mirrors, all traffic received or transmitted on a designated port to a specified mirror port. If a protocol analyzer is attached to the target port, the traffic stream of valid frames on any source port is made available for analysis.



**IMPORTANT!**

Select a target port that has a higher speed than the source port. Mirroring a 100 Mbps port onto a 10 Mbps port may result in an improperly mirrored stream.



**IMPORTANT!**

Frames will be dropped if the full-duplex rate of frames on the source port exceeds the transmission speed of the target port. Since both transmitted and received frames on the source port are mirrored to the target port, frames will be discarded if the sum traffic exceeds the target port's transmission rate. This problem reaches its extreme in the case where traffic on a 100 Mbps full-duplex port is mirrored onto a 10 Mbps half-duplex port.



**IMPORTANT!**

Before configuring port mirroring, note the following:

- Traffic will be mirrored onto the target port irrespective of its VLAN membership. It could be the same as or different from the source port's membership.
- Network management frames (such as RSTP, GVRP etc.) cannot be mirrored.
- Switch management frames generated by the switch (such as Telnet, HTTP, SNMP, etc.) cannot be mirrored.

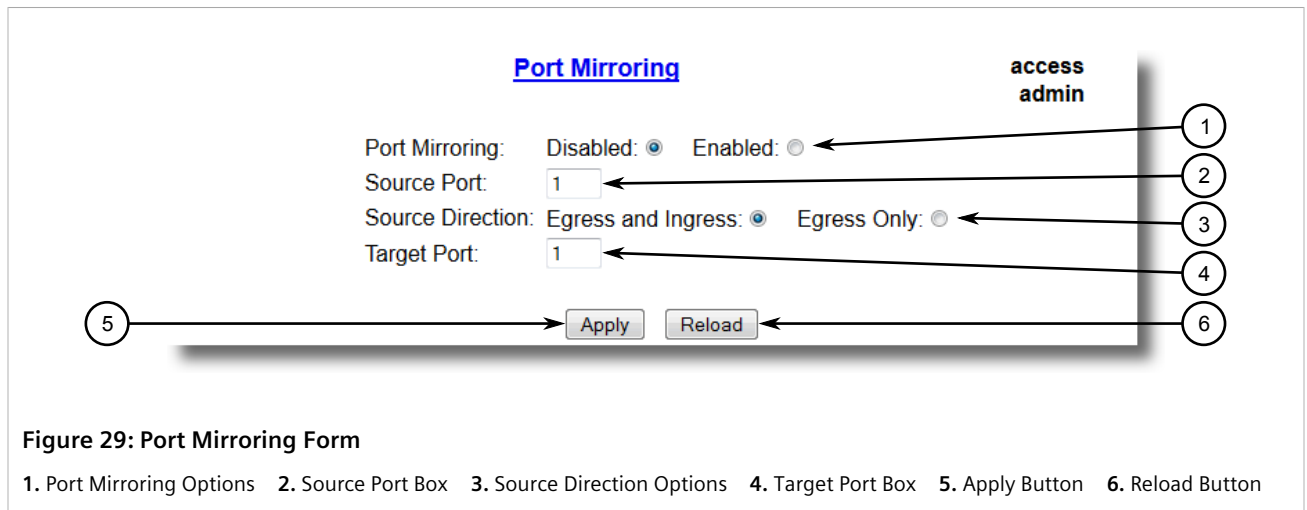


**NOTE**

Invalid frames received on the source port will not be mirrored. These include CRC errors, oversize and undersize packets, fragments, jabbers, collisions, late collisions and dropped events.

To configure port mirroring, do the following:

1. Navigate to **Ethernet Ports » Configure Port Mirroring**. The **Port Mirroring** form appears.



**Figure 29: Port Mirroring Form**

1. Port Mirroring Options
2. Source Port Box
3. Source Direction Options
4. Target Port Box
5. Apply Button
6. Reload Button

2. Configure the following parameter(s) as required:

Parameter	Description
Port Mirroring	<b>Synopsis:</b> { Disabled, Enabled } <b>Default:</b> Disabled Enabling port mirroring causes all frames received and transmitted by the source port(s) to be transmitted out of the target port.
Source Port	<b>Synopsis:</b> Any combination of numbers valid for this parameter The port(s) being monitored.
Source Direction	<b>Synopsis:</b> Egress and Ingress, Egress Only <b>Default:</b> Egress and Ingress Specifies monitoring whether both egress and ingress traffics or only egress traffic of the source port.
Target Port	<b>Synopsis:</b> 1 to maximum port number <b>Default:</b> 1 The port where a monitoring device should be connected.

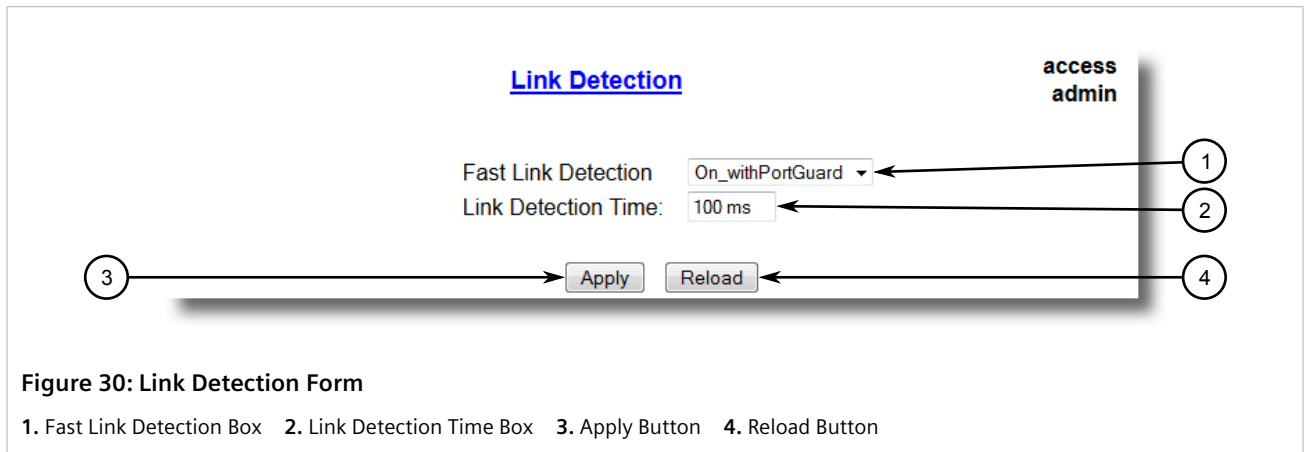
3. Click **Apply**.

Section 4.6.9

## Configuring Link Detection

To configure link detection, do the following:

1. Navigate to **Ethernet Ports » Configure Link Detection**. The **Link Detection** form appears.



2. Configure the following parameter(s) as required:

**NOTE**  
When Fast Link Detection is enabled, the system prevents link state change processing from consuming all available CPU resources. However, if Port Guard is not used, it is possible for almost all available CPU time to be consumed by frequent link state changes, which could have a negative impact on overall system responsiveness.

Parameter	Description
Fast Link Detection	<b>Synopsis:</b> { Off, On, On_withPortGuard } <b>Default:</b> On_withPortGuard

Parameter	Description
	<p>This parameter provides protection against faulty end devices generating an improper link integrity signal. When a faulty end device or a mis-matching fiber port is connected to the unit, a large number of continuous link state changes could be reported in a short period of time. These large number of bogus link state changes could render the system unresponsive as most, if not all, of the system resources are used to process the link state changes. This could in turn cause a serious network problem as the unit's RSTP process may not be able to run, thus allowing network loop to form.</p> <p>Three different settings are available for this parameter:</p> <ul style="list-style-type: none"> <li>• <b>ON_withPortGuard</b> - This is the recommended setting. With this setting, an extended period (~2 minutes) of excessive link state changes reported by a port will prompt Port Guard feature to disable FAST LINK DETECTION on that port and raise an alarm. By disabling FAST LINK DETECTION on the problematic port, excessive link state changes can no longer consume substantial amount of system resources. However if FAST LINK DETECTION is disabled, the port will need a longer time to detect a link failure. This may result in a longer network recovery time of up to 2s. Once Port Guard disables FAST LINK DETECTION of a particular port, user can re-enable FAST LINK DETECTION on the port by clearing the alarm.</li> <li>• <b>ON</b> - In certain special cases where a prolonged excessive link state changes constitute a legitimate link operation, using this setting can prevent Port Guard from disabling FAST LINK DETECTION on the port in question. If excessive link state changes persist for more than 2 minutes, an alarm will be generated to warn user about the observed bouncing link. If the excessive link state changes condition is resolved later on, the alarm will be cleared automatically. Since this option does not disable FAST LINK DETECTION, a persistent bouncing link could continue affect the system in terms of response time. This setting should be used with caution.</li> <li>• <b>OFF</b> - Turning this parameter OFF will disable FAST LINK DETECTION completely. The switch will need a longer time to detect a link failure. This will result in a longer network recovery time of up to 2s.</li> </ul>
Link Detection Time	<p><b>Synopsis:</b> 100 ms to 1000 ms <b>Default:</b> 100 ms</p> <p>The time that the link has to continuously stay up before the "link up" decision is made by the device.</p> <p>(The device performs de-bouncing of Ethernet link detection to avoid multiple responses to an occasional link bouncing event, e.g. when a cable is shaking while being plugged-in or unplugged).</p>

3. Click **Apply**.

Section 4.6.10

## Managing SFP Transceivers

RUGGEDCOM ROS supports Small Form-factor Pluggable (SFP) transceivers to provide a 1000Base-X, 100Base-FX, 1000Base-T or 100Base-TX link.



**NOTE**

Since 1000Base-X fiber SFP transceivers are standardized, RUGGEDCOM ROS supports most models of this type. For more information, refer to the [RUGGEDCOM SFP Transceivers Catalog \[https://support.industry.siemens.com/cs/ww/en/view/109482309\]](https://support.industry.siemens.com/cs/ww/en/view/109482309).

*It is strongly recommended to use SFP transceiver models approved by Siemens only. Siemens performs extensive testing on these transceivers to make sure they can withstand harsh conditions. If a different SFP transceiver model is used, it is the user's responsibility to verify it meets environmental and usage requirements.*

*1000Base-T copper SFP transceivers are not standardized. RUGGEDCOM ROS supports only selected models of this type.*

**NOTE**  
SFP transceivers are hot swappable.

When an SFP transceiver is inserted in to the SFP cage, the speed and auto-negotiation settings for the port are automatically adjusted to the appropriate values. For example, if a 1 G SFP transceiver is installed, the speed of the port is automatically changed to 1 G and auto-negotiation is set to **On**.

**CONTENTS**

- [Section 4.6.10.1, "SFP Transceiver Requirements"](#)
- [Section 4.6.10.2, "Monitoring an SFP Port"](#)
- [Section 4.6.10.3, "Displaying Information for an SFP Port"](#)

Section 4.6.10.1

## SFP Transceiver Requirements

Depending on the required link media type, an SFP port may require some explicit configuration:

- For 100Base-FX or 100Base-TX links, the speed must be set to 100 Mbps.
- For 1000Base-X or 1000Base-T links, the speed of the SFP port must be set to 1 Gbps.
- Auto-negotiation can be configured to *On* when the port speed is set to 1 Gbps, or to *Off* when the port speed is set to 100 Mbps.
- Duplex mode cannot be configured on an SFP port and is always forced to full duplex.

For more information about configuring SFP transceiver ports and other Ethernet ports on the device, refer to [Section 4.6.6, "Configuring an Ethernet Port"](#).

Section 4.6.10.2

## Monitoring an SFP Port

RUGGEDCOM ROS supports hot-swapping of SFP transceivers on SFP ports and will automatically detect when an SFP transceiver is removed or installed.

When RUGGEDCOM ROS detects that an SFP transceiver is plugged into an SFP port, it reads the transceiver information and determines the transceiver type. This decision results in RUGGEDCOM ROS either *accepting*, *accepting and reconfiguring*, or *rejecting* the SFP port.

The following table shows in which cases an SFP transceiver is *accepted* or *accepted and reconfigured*.

Configured Speed	Detected SFP Type: 1000Base-X	Detected SFP Type: 100Base-FX	Detected SFP Type: 1000Base-T
1 Gbps	Accept	Accept and automatically set the speed to 100 Mbps and set auto-negotiation to <i>Off</i>	Accept
100 Mbps	Accept and automatically set the speed to 1 Gbps and set auto-negotiation to <i>On</i>	Accept	Compare the transceiver model against a list of supported models. Accept if it is in the list. Otherwise, automatically

Configured Speed	Detected SFP Type: 1000Base-X	Detected SFP Type: 100Base-FX	Detected SFP Type: 1000Base-T
			set the speed to 1 Gbps and set auto-negotiation to <i>On</i> .

If the transceiver is *accepted*, the *Media* parameter under **Ethernet Ports » Configure Port Parameters** shows detailed information about the SFP transceiver, including Gigabit Ethernet Compliance Code, transmission media, connector type, and link length. For example:

```
SFP 1000LX SM LC 10 km
SFP 1000T 100 m
```

If the transceiver is not recognized, it is *rejected*. An alarm is also generated and the port is blocked so that no link can be established until the transceiver is replaced. The *Media* parameter shows the rejected SFP transceiver is unidentified. For example:

```
SFP Unidentified
```

If no transceiver is installed on an SFP port, the *Media* parameter shows the SFP transceiver is unplugged:

```
SFP Unplugged
```

### Section 4.6.10.3

## Displaying Information for an SFP Port

To display detailed information about an SFP port, do the following:

1. Log in to the device and access the CLI shell. For more information about accessing the CLI shell, refer to [Section 2.5, "Using the Command Line Interface"](#).
2. Type the following command:

```
sfp port
```

Where:

- *port* is the port number

Information about the SFP port is displayed. For example:

```
>sfp 1
ID: SFP
Extended ID: GBIC/SFP function is defined by serial ID only
Connector: LC
Transceiver:
Gigabit Ethernet Compliance Codes:
1000LX
Fibre Channel link length:
Long Distance (L)
Fibre Channel transmitter technology:
Longwave laser (LC)
Fibre Channel transmission media:
Single Mode (SM)
Fibre Channel speed:
100 MBytes/Sec
Baud Rate, nominal: 1300 MBits/sec
Encoding type: 8B10B
Length(9um): 10 km
Length(9um): 10000 m
Length(50um): 550 m
Length(62.5um): 550 m
Length(Copper): Not specified
```

```
Vendor: xxxxxxxx
IEEE company ID: xxxxxxxx
Part number: xxxxxxxxxxxx
Revision: 0000
Laser wavelength: 1310 nm
>
```

## Section 4.6.11

## Managing PoE Ports

The RUGGEDCOM RS900GPF features eight IEEE 802.3at compliant Power over Ethernet (POE) ports powered by an external power supply. Through RUGGEDCOM ROS, these ports can be managed as follows:

- **Overload Protection**  
Prioritize and automatically enable/disable the lowest priority ports depending on power demands.
- **Power Conservation**  
Schedule ports to enable/disable automatically at specific times during the week to conserve power.

For more information about the PoE ports, refer to the *RUGGEDCOM RS900GPF Installation Guide*.

### CONTENTS

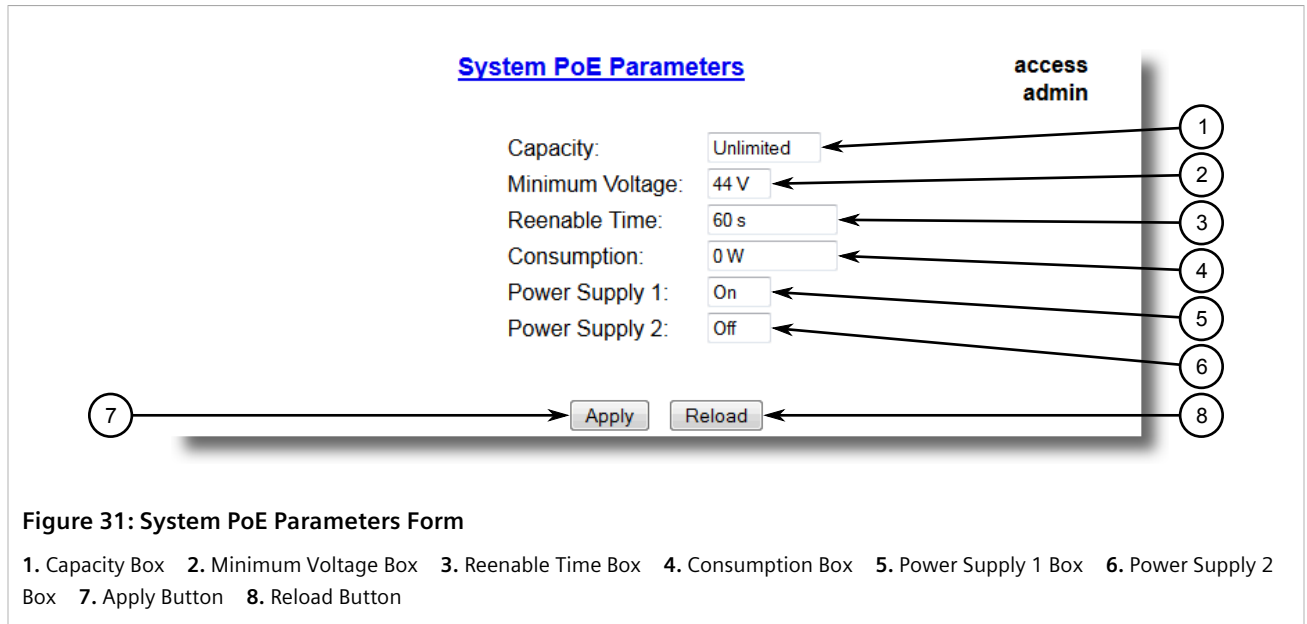
- [Section 4.6.11.1, "Configuring PoE Ports Globally"](#)
- [Section 4.6.11.2, "Configuring a Specific PoE Port"](#)
- [Section 4.6.11.3, "Scheduling PoE Ports"](#)

## Section 4.6.11.1

### Configuring PoE Ports Globally

To configure global settings for all Power-over-Ethernet (PoE) ports, do the following:

1. Navigate to **Ethernet Ports » Configure/View PoE Parameters » Configure/View System PoE Parameters**. The **System PoE Parameters** form appears.



**Figure 31: System PoE Parameters Form**

1. Capacity Box 2. Minimum Voltage Box 3. Reenable Time Box 4. Consumption Box 5. Power Supply 1 Box 6. Power Supply 2 Box 7. Apply Button 8. Reload Button

2. Configure the following parameter(s) as required:

Parameter	Description
Capacity	<p><b>Synopsis:</b> 1 to 400 W or { Unlimited }</p> <p><b>Default:</b> Unlimited</p> <p>The capacity of the PoE power supply source. That is, the maximum total output power can be provided by all PoE ports.</p> <p>When total power consumption reached this limit, some ports will be shutdown.</p> <p>If set to Unlimited, the total output power is not limited by software.</p>
Minimum Voltage	<p><b>Synopsis:</b> 39 to 57 V</p> <p><b>Default:</b> 44 V</p> <p>The minimum required voltage for PoE ports.</p> <p>If PoE voltage dropped below this threshold, some ports will be shutdown.</p> <p>The IEEE 802.3af standard specifies the PoE voltage range as 44 - 57 V.</p> <p>The IEEE 802.3at standard specifies the PoE voltage range as 50 - 57 V.</p>
Reenable Time	<p><b>Synopsis:</b> 10 to 4294967295 s</p> <p><b>Default:</b> 60 s</p> <p>The time to wait to turn on PoE ports again after they were shutdown due to overload condition.</p>
Consumption	<p><b>Synopsis:</b> 0 to 4294967295 W</p> <p>Current total power consumption by all PoE devices.</p>

3. Click **Apply**.

#### Section 4.6.11.2

### Configuring a Specific PoE Port

To configure Power-over-Ethernet (PoE) settings for a specific Ethernet port, do the following:



1. Navigate to **Ethernet Ports » Configure/View PoE Parameters » Configure/View Port PoE Parameters**. The **Port PoE Parameters** table appears.

Port	Admin	Compliant	Priority	Powered	Class	Voltage	Current
<a href="#">1</a>	Enabled	Yes	Normal	No	0	0 V	0 mA
<a href="#">2</a>	Enabled	Yes	Normal	No	0	0 V	0 mA
<a href="#">3</a>	Enabled	Yes	Normal	No	0	0 V	0 mA
<a href="#">4</a>	Enabled	Yes	Normal	No	0	0 V	0 mA
<a href="#">5</a>	Enabled	Yes	Normal	No	0	0 V	0 mA
<a href="#">6</a>	Enabled	Yes	Normal	No	0	0 V	0 mA
<a href="#">7</a>	Enabled	Yes	Normal	No	0	0 V	0 mA
<a href="#">8</a>	Enabled	Yes	Normal	No	0	0 V	0 mA

access  
admin

Figure 32: Port PoE Parameters Table

2. Select an Ethernet port. The **Port PoE Parameters** form appears.

**Port PoE Parameters**

access  
admin

Port:  ← 1

Admin: Disabled:  Enabled:  ← 2

Compliant: No:  Yes:  ← 3

Priority: Normal:  Low:  ← 4

Powered:  ← 5

Class:  ← 6

Voltage:  ← 7

Current:  ← 8

← 9  ← 10

Figure 33: Port PoE Parameters Form

1. Port Box 2. Admin Options 3. Compliant Options 4. Priority Options 5. Powered Box 6. Class Box 7. Voltage Box  
8. Current Box 9. Apply Button 10. Reload Button

3. Configure the following parameter(s) as required:

Parameter	Description
Port	<b>Default:</b> 1 The port number as seen on the front plate silkscreen of the switch.
Admin	<b>Synopsis:</b> { Disabled, Enabled } <b>Default:</b> Enabled This parameter allows to enable or disable supplying power by the port.
Compliant	<b>Synopsis:</b> { No, Yes } <b>Default:</b> Yes Set this value to Yes (default) if the attached powered device is compliant to the IEEE802.3at/IEEE802.3af standard.

Parameter	Description
	Set this value to No if the attached device is a non-standard compliant PoE device such as the RUGGEDCOM WIN7200. In this case, power to the port is forced on without performing a signature test.
Priority	<b>Synopsis:</b> { Normal, Low } <b>Default:</b> Normal  Specify whether this port is of low priority. Low priority ports will be shutdown first if power supply is overloaded. Other ports may be shutdown as well if overload condition still exists after shutting down low priority ports.
Powered	<b>Synopsis:</b> { No, Yes }  Whether or not power is currently supplied by the port.
Class	<b>Synopsis:</b> 0 to 65535  PoE Class value that defines the minimum supplied power level. For more information, refer to the IEEE 802.1af and 802.1at standards. 0 = 15.4 W (default) 1 = 4.0 W 2 = 7.0 W 3 = 15.4 W 4 = 34.2 W
Voltage	<b>Synopsis:</b> 0 to 65535  Supplied voltage level.
Current	<b>Synopsis:</b> 0 to 65535  Supplied current level.

4. Click **Apply**.

Section 4.6.11.3

## Scheduling PoE Ports

To save power, Power-over-Ethernet (PoE) ports can be configured to shut down and restart at specific times during the week.

To configure a schedule for when a PoE port should be powered on, do the following:

1. Navigate to **Ethernet Ports » Configure/View PoE Parameters » Configure PoE Scheduling**. The **PoE Scheduling** table appears.

**PoE Scheduling**

**access  
admin**

Port	Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
1	05:00 24	17:00 12	17:00 12	17:00 12	17:00 12	17:00 24	05:00 24
2	05:00 24	17:00 12	17:00 12	17:00 12	17:00 12	17:00 24	05:00 24
3	05:00 24	17:00 12	17:00 12	17:00 12	17:00 12	17:00 24	05:00 24
4	05:00 24	17:00 12	17:00 12	17:00 12	17:00 12	17:00 24	05:00 24
5	05:00 24	17:00 12	17:00 12	17:00 12	17:00 12	17:00 24	05:00 24
6	05:00 24	17:00 12	17:00 12	17:00 12	17:00 12	17:00 24	05:00 24
7	05:00 24	17:00 12	17:00 12	17:00 12	17:00 12	17:00 24	05:00 24
8	05:00 24	17:00 12	17:00 12	17:00 12	17:00 12	17:00 24	05:00 24

Figure 34: PoE Scheduling Table

2. Select an Ethernet port. The **PoE Scheduling** form appears.

**PoE Scheduling**

**access  
admin**

Port:

Sunday:

Monday:

Tuesday:

Wednesday:

Thursday:

Friday:

Saturday:

Figure 35: PoE Scheduling Form

1. Port Box 2. Sunday Box 3. Monday Box 4. Tuesday Box 5. Wednesday Box 6. Thursday Box 7. Friday Box 8. Saturday Box 9. Apply Button 10. Reload Button

3. Configure the following parameter(s) as required:

Parameter	Description
Port	<b>Synopsis:</b> 1 to maximum port number The port number as seen on the front plate silkscreen of the switch.
Sunday	The time period of the day to power off this PoE port to save power. Example: '17:00 12' means that the port will be shut down at 17:00 (5:00PM) for 12 hours. So it will be turned on again at 5:00AM the next day.
Monday	The time period of the day to power off this PoE port to save power. Example: '17:00 12' means that the port will be shut down at 17:00 (5:00PM) for 12 hours. So it will be turned on again at 5:00AM the next day.

Parameter	Description
Tuesday	The time period of the day to power off this PoE port to save power. Example: '17:00 12' means that the port will be shut down at 17:00 (5:00PM) for 12 hours. So it will be turned on again at 5:00AM the next day.
Wednesday	The time period of the day to power off this PoE port to save power. Example: '17:00 12' means that the port will be shut down at 17:00 (5:00PM) for 12 hours. So it will be turned on again at 5:00AM the next day.
Thursday	The time period of the day to power off this PoE port to save power. Example: '17:00 12' means that the port will be shut down at 17:00 (5:00PM) for 12 hours. So it will be turned on again at 5:00AM the next day.
Friday	The time period of the day to power off this PoE port to save power. Example: '17:00 12' means that the port will be shut down at 17:00 (5:00PM) for 12 hours. So it will be turned on again at 5:00AM the next day.
Saturday	The time period of the day to power off this PoE port to save power. Example: '17:00 12' means that the port will be shut down at 17:00 (5:00PM) for 12 hours. So it will be turned on again at 5:00AM the next day.

- Click **Apply**.

#### Section 4.6.12

## Detecting Cable Faults

Connectivity issues can sometimes be attributed to faults in Ethernet cables. To help detect cable faults, short circuits, open cables or cables that are too long, RUGGEDCOM ROS includes a built-in cable diagnostics utility.

### CONTENTS

- [Section 4.6.12.1, "Viewing Cable Diagnostics Results"](#)
- [Section 4.6.12.2, "Performing Cable Diagnostics"](#)
- [Section 4.6.12.3, "Clearing Cable Diagnostics"](#)
- [Section 4.6.12.4, "Determining the Estimated Distance To Fault \(DTF\)"](#)

#### Section 4.6.12.1

### Viewing Cable Diagnostics Results

To view the results of previous diagnostic tests, navigate to **Ethernet Ports » Configure/View Cable Diagnostics Parameters**. The **Cable Diagnostics Parameters** table appears.



**NOTE**

For information about how to start a diagnostic test, refer to [Section 4.6.12.2, "Performing Cable Diagnostics"](#).

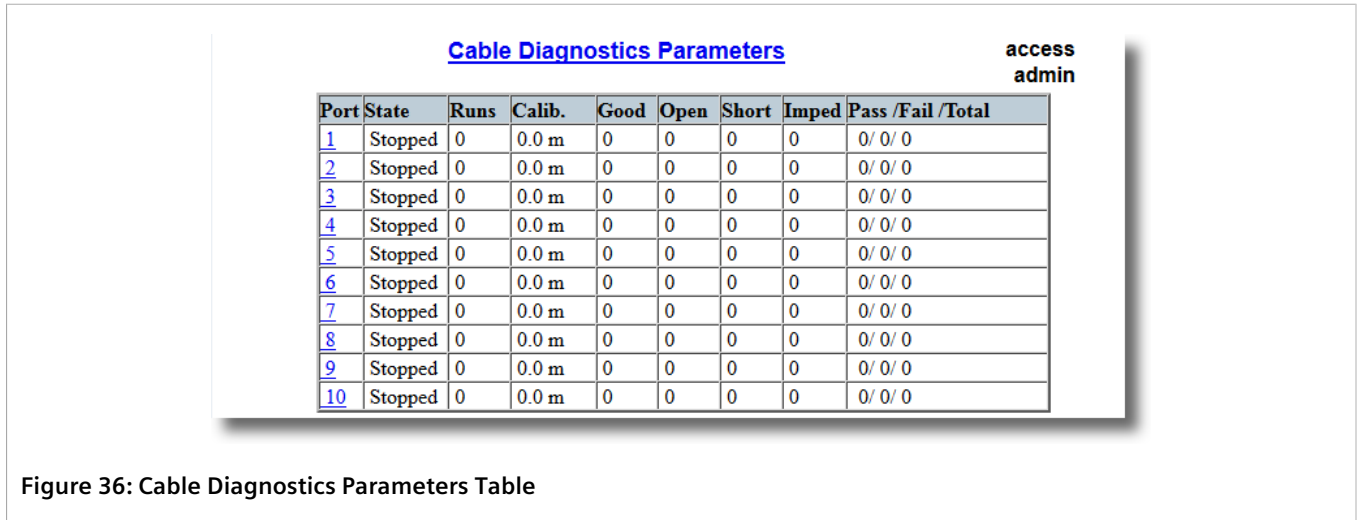


Figure 36: Cable Diagnostics Parameters Table

This table displays the following information:

Parameter	Description
Port	<b>Synopsis:</b> 1 to maximum port number The port number as seen on the front plate silkscreen of the switch.
State	<b>Synopsis:</b> { Stopped, Started } Control the start/stop of the cable diagnostics on the selected port. If a port does not support cable diagnostics, State will be reported as N/A.
Runs	<b>Synopsis:</b> 0 to 65535 The total number of times cable diagnostics to be performed on the selected port. If this number is set to 0, cable diagnostics will be performed forever on the selected port.
Calib.	<b>Synopsis:</b> -100.0 to 100.0 m This calibration value can be used to adjust or calibrate the estimated distance to fault. User can take following steps to calibrate the cable diagnostics estimated distance to fault: <ul style="list-style-type: none"> <li>• Pick a particular port which calibration is needed</li> <li>• Connect an Ethernet cable with a known length (e.g. 50m) to the port</li> <li>• DO NOT connect the other end of the cable to any link partner</li> <li>• Run cable diagnostics a few times on the port. OPEN fault should be detected</li> <li>• Find the average distance to the OPEN fault recorded in the log and compare it to the known length of the cable. The difference can be used as the calibration value</li> <li>• Enter the calibration value and run cable diagnostics a few more times</li> <li>• The distance to OPEN fault should now be at similar distance as the cable length</li> <li>• Distance to fault for the selected port is now calibrated</li> </ul>
Good	<b>Synopsis:</b> 0 to 65535 The number of times GOOD TERMINATION (no fault) is detected on the cable pairs of the selected port.
Open	<b>Synopsis:</b> 0 to 65535 The number of times OPEN is detected on the cable pairs of the selected port.
Short	<b>Synopsis:</b> 0 to 65535

Parameter	Description
	The number of times SHORT is detected on the cable pairs of the selected port.
Imped	<b>Synopsis:</b> 0 to 65535 The number of times IMPEDANCE MISMATCH is detected on the cable pairs of the selected port.
Pass /Fail /Total	<b>Synopsis:</b> Any 19 characters This field summarizes the results of the cable diagnostics performed so far. Pass - number of times cable diagnostics successfully completed on the selected port. Fail - number of times cable diagnostics failed to complete on the selected port. Total - total number of times cable diagnostics have been attempted on the selected port.



**NOTE**

*For each successful diagnostic test, the values for **Good**, **Open**, **Short** or **Imped** will increment based on the number of cable pairs connected to the port. For a 100Base-T port, which has two cable pairs, the number will increase by two. For a 1000Base-T port, which has four cable pairs, the number will increase by four.*



**NOTE**

*When a cable fault is detected, an estimated distance-to-fault is calculated and recorded in the system log. The log lists the cable pair, the fault that was detected, and the distance-to-fault value. For more information about the system log, refer to [Section 4.5.1, "Viewing Local and System Logs"](#).*

Section 4.6.12.2

## Performing Cable Diagnostics

To perform a cable diagnostic test on one or more Ethernet ports, do the following:

1. Connect a CAT-5 (or better quality) Ethernet cable to the selected Ethernet port.



**IMPORTANT!**

*Both the selected Ethernet port and its partner port can be configured to run in **Enabled** mode with auto-negotiation, or in **Disabled** mode. Other modes are not recommended, as they may interfere with the cable diagnostics procedure.*

2. Connect the other end of the cable to a similar network port. For example, connect a 100Base-T port to a 100Base-T port, or a 1000Base-T port to a 1000Base-T port.
3. In RUGGEDCOM ROS, navigate to **Ethernet Ports » Configure/View Cable Diagnostics Parameters**. The **Cable Diagnostics Parameters** table appears.

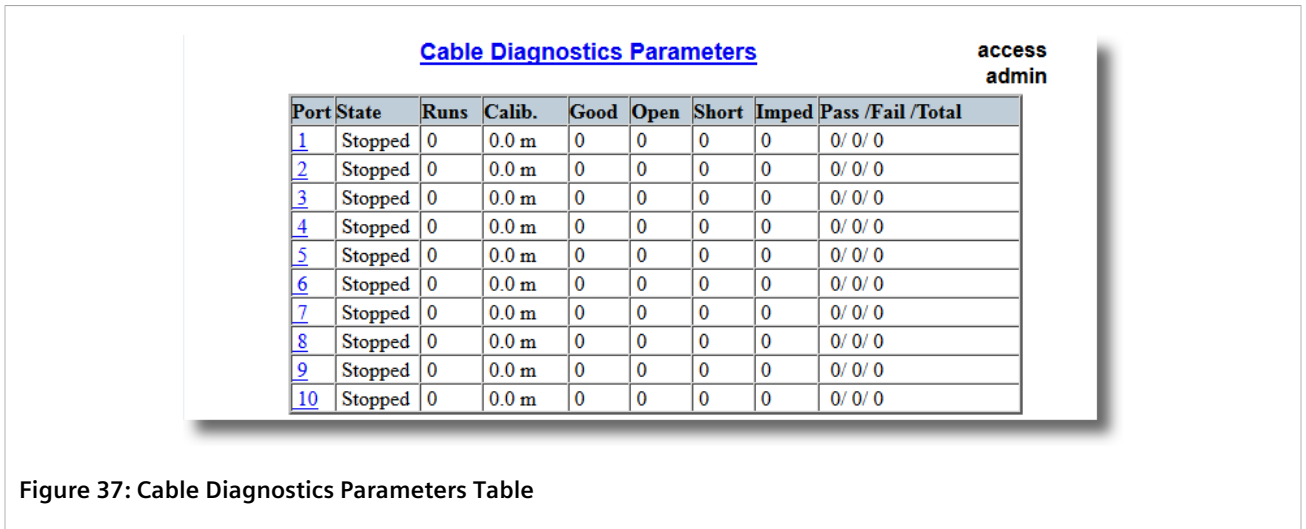


Figure 37: Cable Diagnostics Parameters Table

- Select an Ethernet port. The **Cable Diagnostics Parameters** form appears.

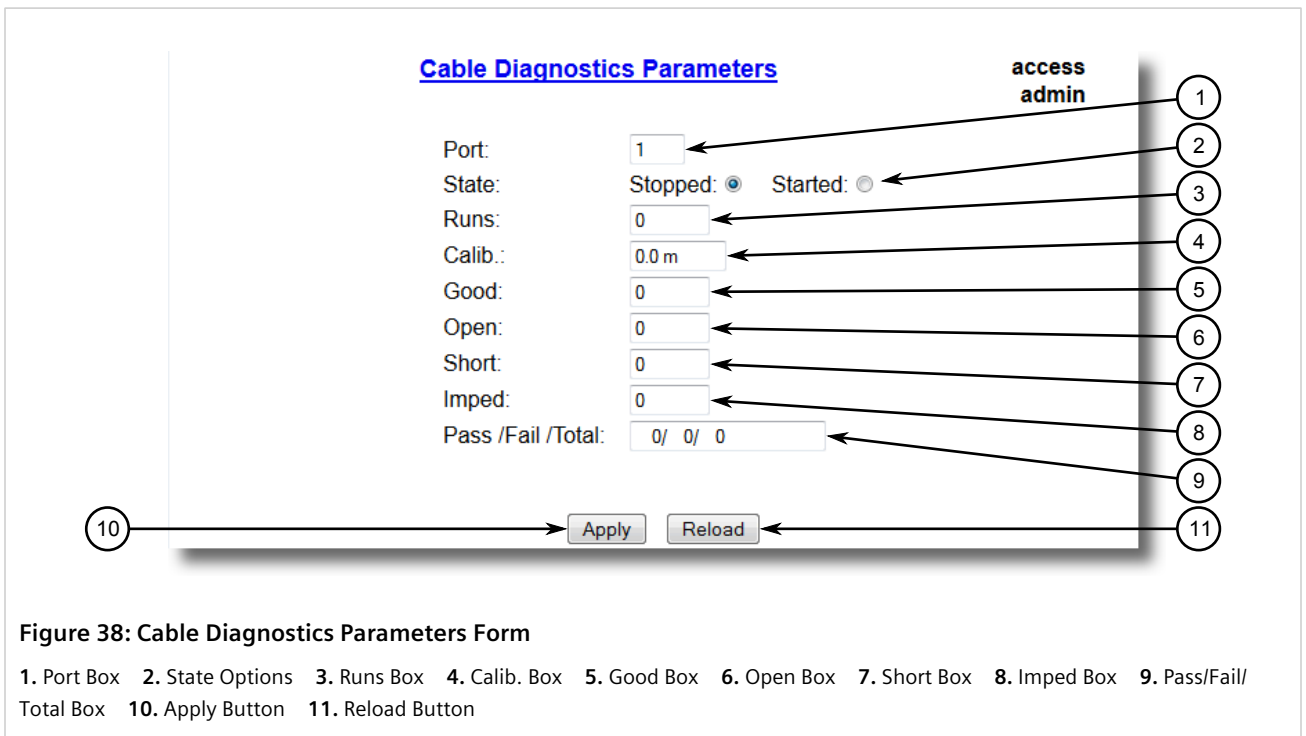


Figure 38: Cable Diagnostics Parameters Form

1. Port Box 2. State Options 3. Runs Box 4. Calib. Box 5. Good Box 6. Open Box 7. Short Box 8. Imped Box 9. Pass/Fail/Total Box 10. Apply Button 11. Reload Button

- Under **Runs**, enter the number of consecutive diagnostic tests to perform. A value of 0 indicates the test will run continuously until stopped by the user.
- Under **Calib.**, enter the estimated Distance To Fault (DTF) value. For information about how to determine the DTF value, refer to [Section 4.6.12.4, "Determining the Estimated Distance To Fault \(DTF\)"](#).
- Select **Started**.

**IMPORTANT!**  
A diagnostic test can be stopped by selecting **Stopped** and clicking **Apply**. However, if the test is stopped in the middle of a diagnostic run, the test will run to completion.

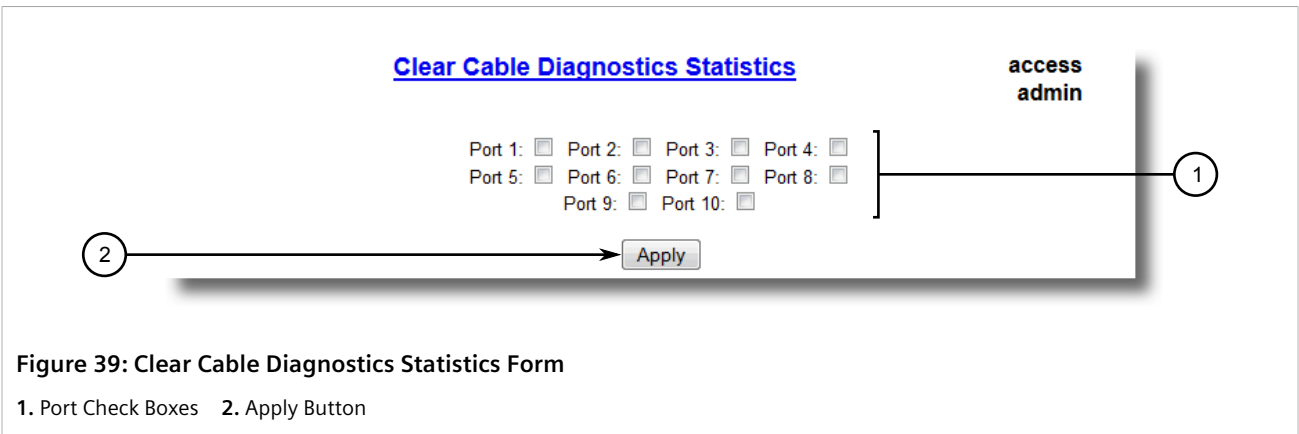
- Click **Apply**. The state of the Ethernet port will automatically change to *Stopped* when the test is complete. For information about how to monitor the test and view the results, refer to [Section 4.6.12.1, "Viewing Cable Diagnostics Results"](#).

### Section 4.6.12.3

## Clearing Cable Diagnostics

To clear the cable diagnostic results, do the following:

- Navigate to **Ethernet Ports » Clear Cable Diagnostics Statistics**. The **Clear Cable Diagnostics Statistics** form appears.



- Select one or more Ethernet ports.
- Click **Apply**.

### Section 4.6.12.4

## Determining the Estimated Distance To Fault (DTF)

To determine the estimate Distance To Fault (DTF), do the following:

- Connect a CAT-5 (or better quality) Ethernet cable with a known length to the device. Do not connect the other end of the cable to another port.
- Configure the cable diagnostic utility to run a few times on the selected Ethernet port and start the test. For more information, refer to [Section 4.6.12.2, "Performing Cable Diagnostics"](#). Open faults should be detected and recorded in the system log.
- Review the errors recorded in the system log and determine the average distance of the open faults. For more information about the system log, refer to [Section 4.5.1, "Viewing Local and System Logs"](#).
- Subtract the average distance from the cable length to determine the calibration value.
- Configure the cable diagnostic utility to run a few times with the new calibration value. The distance to the open fault should now be the same as the actual length of the cable. The Distance To Fault (DTF) is now calibrated for the selected Ethernet port.



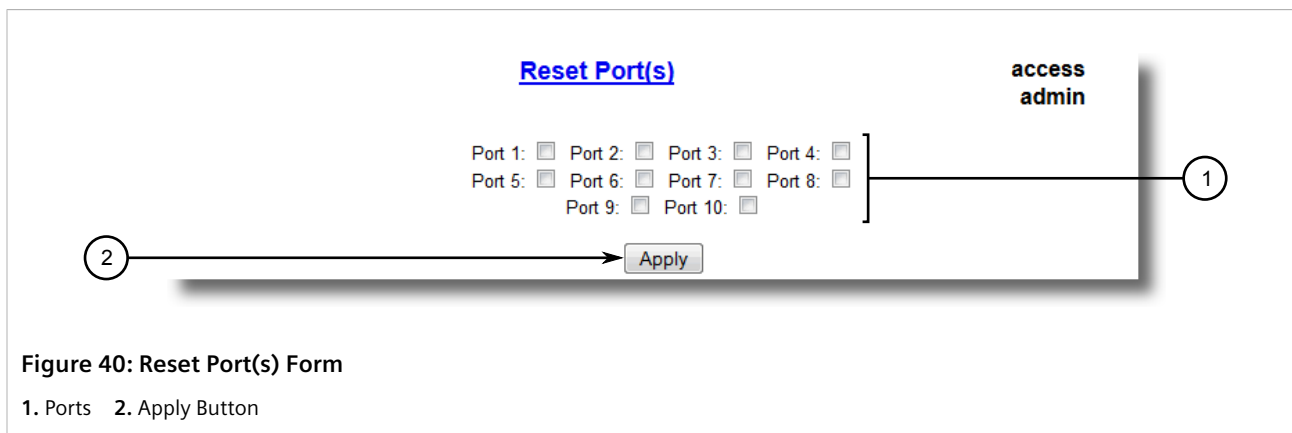
## Section 4.6.13

## Resetting Ethernet Ports

At times, it may be necessary to reset a specific Ethernet port, such as when the link partner has latched into an inappropriate state. This is also useful for forcing a re-negotiation of the speed and duplex modes.

To reset a specific Ethernet port(s), do the following:

1. Navigate to **Ethernet Ports** » **Reset Port(s)**. The **Reset Port(s)** form appears.



2. Select one or more Ethernet ports to reset.
3. Click **Apply**. The selected Ethernet ports are reset.

## Section 4.7

## Managing IP Interfaces

RUGGEDCOM ROS allows one IP interface to be configured for each subnet (or VLAN), up to a maximum of 255 interfaces. One of the interfaces must also be configured to be a management interface for certain IP services, such as DHCP relay agent.

Each IP interface must be assigned an IP address. In the case of the management interface, the IP address type can be either static, DHCP, BOOTP or dynamic. For all other interfaces, the IP address must be static.

**CAUTION!**

*Configuration hazard – risk of communication disruption. Changing the ID for the management VLAN will break any active Raw Socket TCP connections. If this occurs, reset all serial ports.*

**CONTENTS**

- [Section 4.7.1, “Viewing a List of IP Interfaces”](#)
- [Section 4.7.2, “Adding an IP Interface”](#)
- [Section 4.7.3, “Deleting an IP Interface”](#)

Section 4.7.1

## Viewing a List of IP Interfaces

To view a list of IP interfaces configured on the device, navigate to **Administration » Configure IP Interfaces » Configure IP Interfaces**. The **IP Interfaces** table appears.

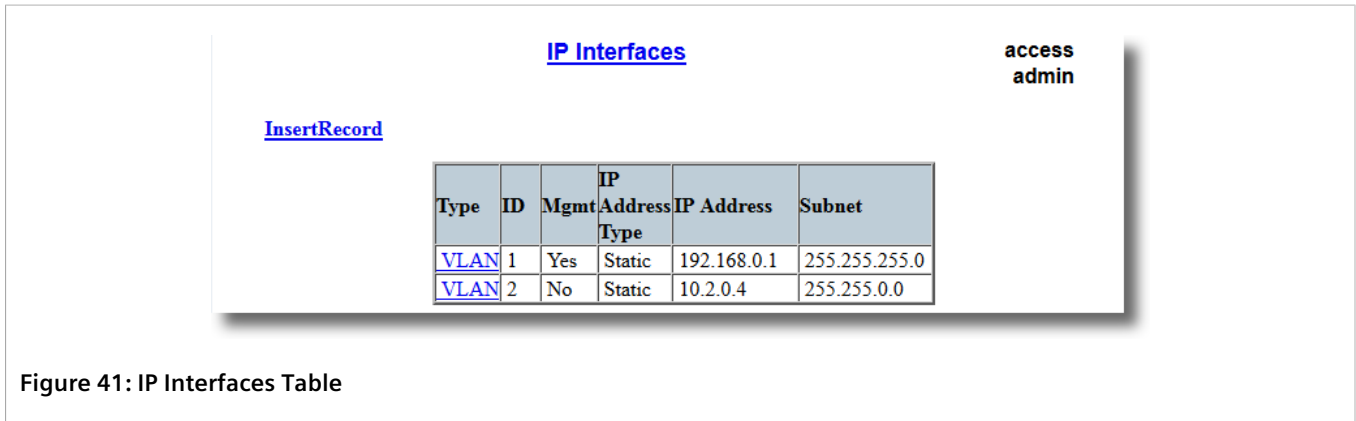


Figure 41: IP Interfaces Table

If IP interfaces have not been configured, add IP interfaces as needed. For more information, refer to [Section 4.7.2, "Adding an IP Interface"](#).

Section 4.7.2

## Adding an IP Interface

To add an IP interface, do the following:

1. Navigate to **Administration » Configure IP Interfaces**. The **IP Interfaces** table appears.

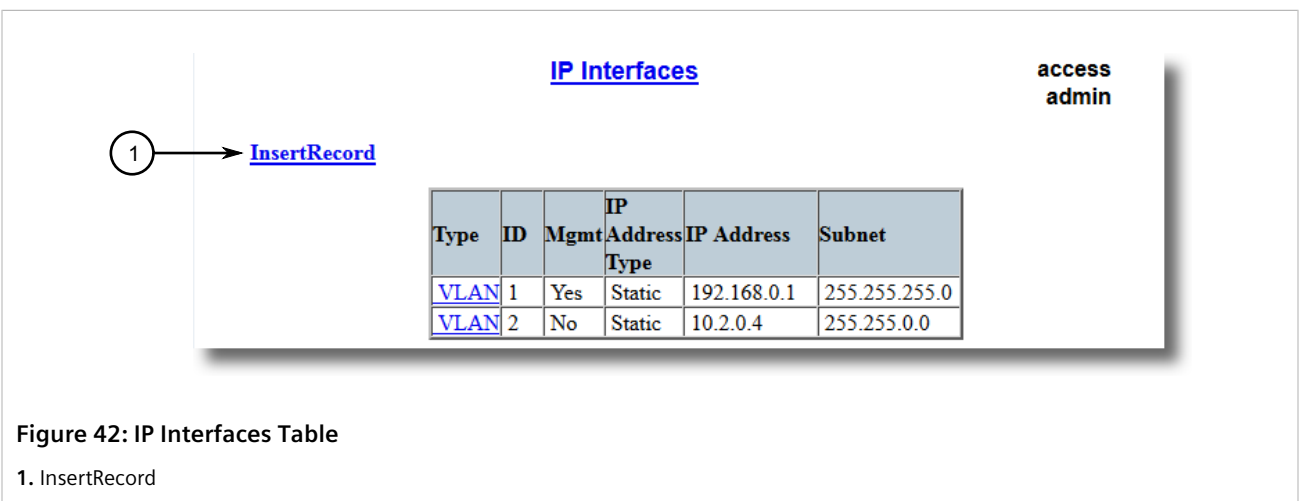
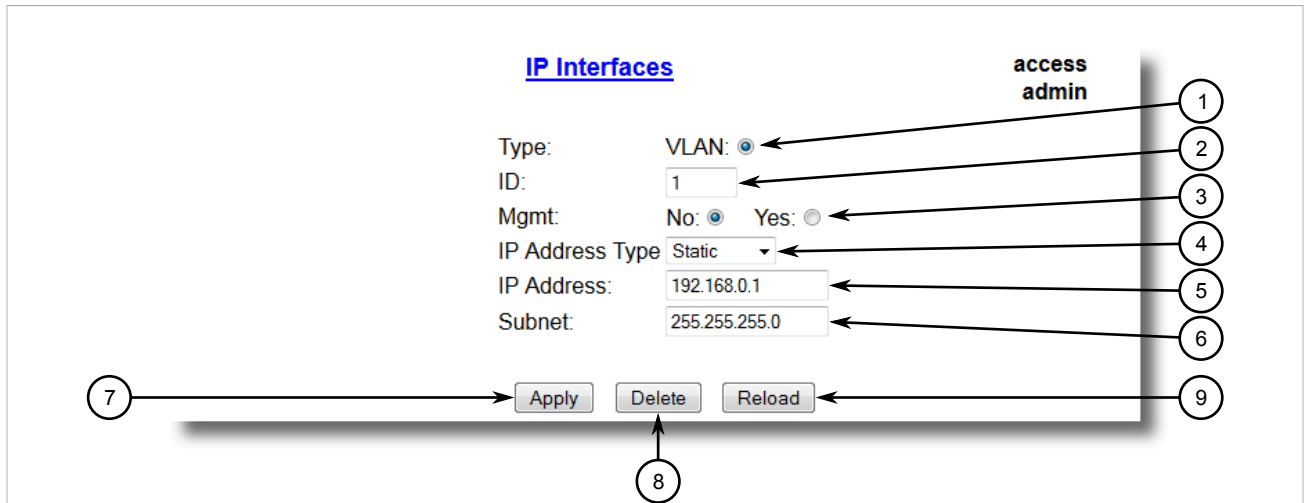


Figure 42: IP Interfaces Table

1. InsertRecord

2. Click **InsertRecord**. The **Switch IP Interfaces** form appears.




**Figure 43: IP Interfaces Form**

- 1. Type Options    2. ID Box    3. Mgmt Options    4. IP Address Type Box    5. IP Address Box    6. Subnet Box    7. Apply Button
- 8. Delete Button    9. Reload Button

3. Configure the following parameter(s) as required:

**NOTE**  
The IP address and mask configured for the management VLAN are not changed when resetting all configuration parameters to defaults and will be assigned a default VLAN ID of 1. Changes to the IP address take effect immediately. All IP connections in place at the time of an IP address change will be lost.

Parameter	Description
Type	<b>Synopsis:</b> { VLAN } <b>Default:</b> VLAN Specifies the type of the interface for which this IP interface is created.
ID	<b>Synopsis:</b> 1 to 4094 <b>Default:</b> 1 Specifies the ID of the interface for which this IP interface is created. If the interface type is VLAN, this represents the VLAN ID.
Mgmt	<b>Synopsis:</b> { No, Yes } <b>Default:</b> No Specifies whether the IP interface is the device management interface.
IP Address Type	<b>Synopsis:</b> { Static, Dynamic, DHCP, BOOTP } <b>Default:</b> Static Specifies whether the IP address is static or is dynamically assigned via DHCP or BOOTP>. The Dynamic option automatically switches between BOOTP and DHCP until it receives a response from the relevant server. The Static option must be used for non-management interfaces.
IP Address	<b>Synopsis:</b> ###.###.###.### where ### ranges from 0 to 255 <b>Default:</b> 192.168.0.1 Specifies the IP address of this device. An IP address is a 32-bit number that is notated by using four numbers from 0 through 255, separated by periods. Only a unicast IP address is allowed, which ranges from 1.0.0.0 to 233.255.255.255.

Parameter	Description
Subnet	<p><b>Synopsis:</b> ###.###.###.### where ### ranges from 0 to 255  <b>Default:</b> 255.255.255.0</p> <p>Specifies the IP subnet mask of this device. An IP subnet mask is a 32-bit number that is notated by using four numbers from 0 through 255, separated by periods. Typically, subnet mask numbers use either 0 or 255 as values (e.g. 255.255.255.0) but other numbers can appear.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;">  <p><b>IMPORTANT!</b> Each IP interface must have a unique network address.</p> </div>

- Click **Apply**.

Section 4.7.3

## Deleting an IP Interface

To delete an IP interface configured on the device, do the following:

- Navigate to **Administration » Configure IP Interfaces**. The **IP Interfaces** table appears.

[IP Interfaces](#)

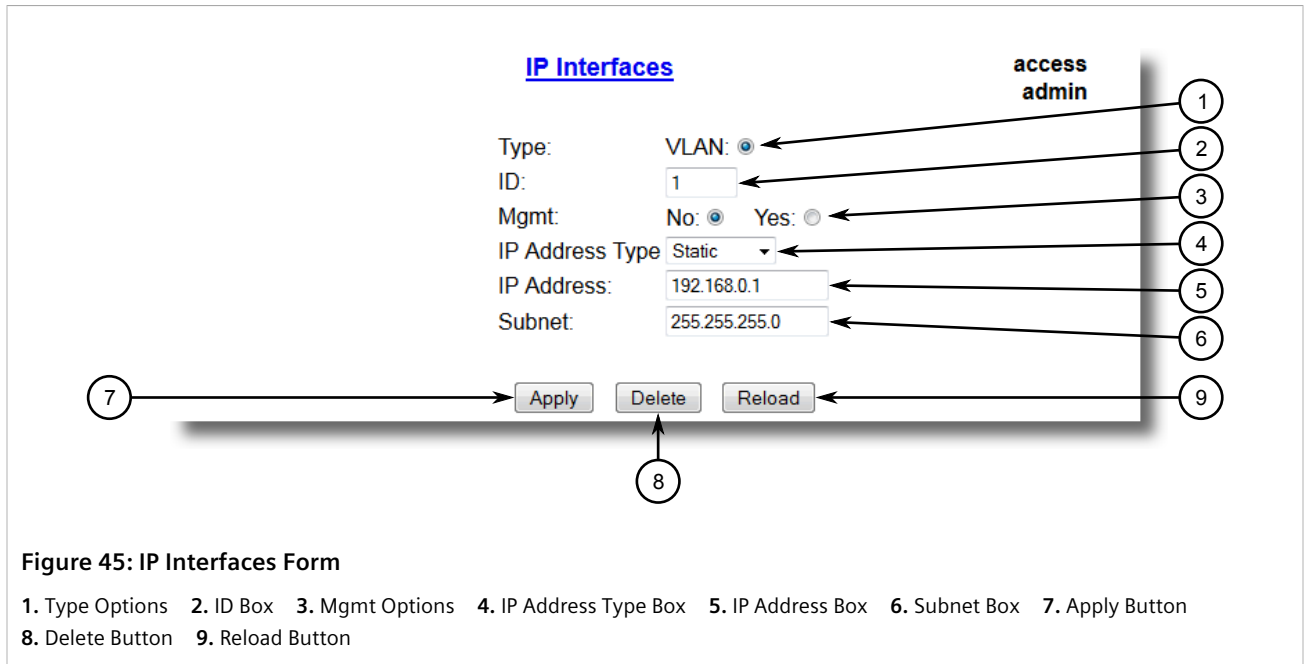
access  
admin

[InsertRecord](#)

Type	ID	Mgmt	IP Address Type	IP Address	Subnet
<a href="#">VLAN</a>	1	Yes	Static	192.168.0.1	255.255.255.0
<a href="#">VLAN</a>	2	No	Static	10.2.0.4	255.255.0.0

**Figure 44: IP Interfaces Table**

- Select the IP interface from the table. The **IP Interfaces** form appears.



3. Click **Delete**.

Section 4.8

## Managing IP Gateways

RUGGEDCOM ROS allows up to ten IP gateways to be configured. When both the **Destination** and **Subnet** parameters are blank, the gateway is considered to be a default gateway.



**NOTE**

*The default gateway configuration will not be changed when resetting all configuration parameters to their factory defaults.*

**CONTENTS**

- [Section 4.8.1, "Viewing a List of IP Gateways"](#)
- [Section 4.8.2, "Adding an IP Gateway"](#)
- [Section 4.8.3, "Deleting an IP Gateway"](#)

Section 4.8.1

### Viewing a List of IP Gateways

To view a list of IP gateways configured on the device, navigate to **Administration » Configure IP Gateways**. The **IP Gateways** table appears.

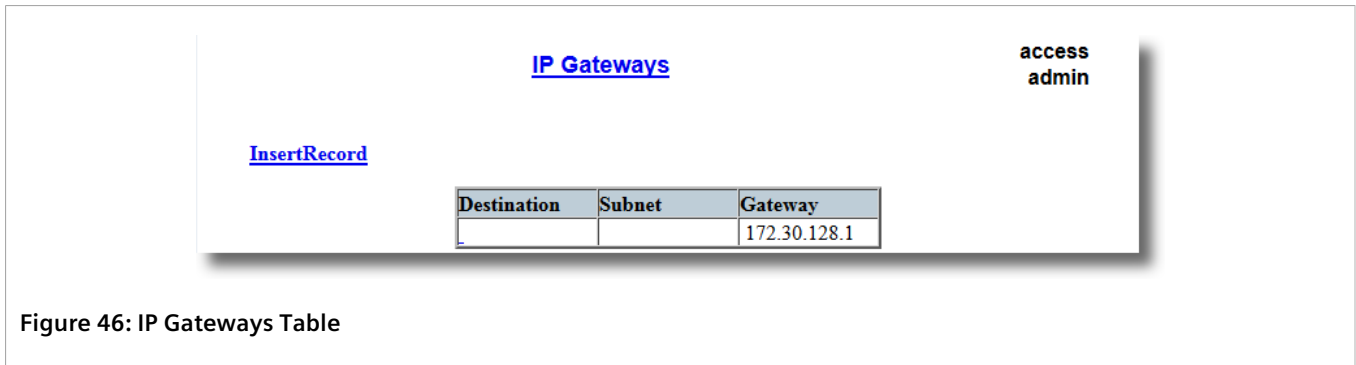


Figure 46: IP Gateways Table

If IP gateways have not been configured, add IP gateways as needed. For more information, refer to [Section 4.8.2, “Adding an IP Gateway”](#).

Section 4.8.2

## Adding an IP Gateway

**IMPORTANT!**  
*DHCP-provided IP gateway addresses will override manually configured values.*

To add an IP gateway, do the following:

1. Navigate to **Administration » Configure IP Gateways**. The **IP Gateways** table appears.

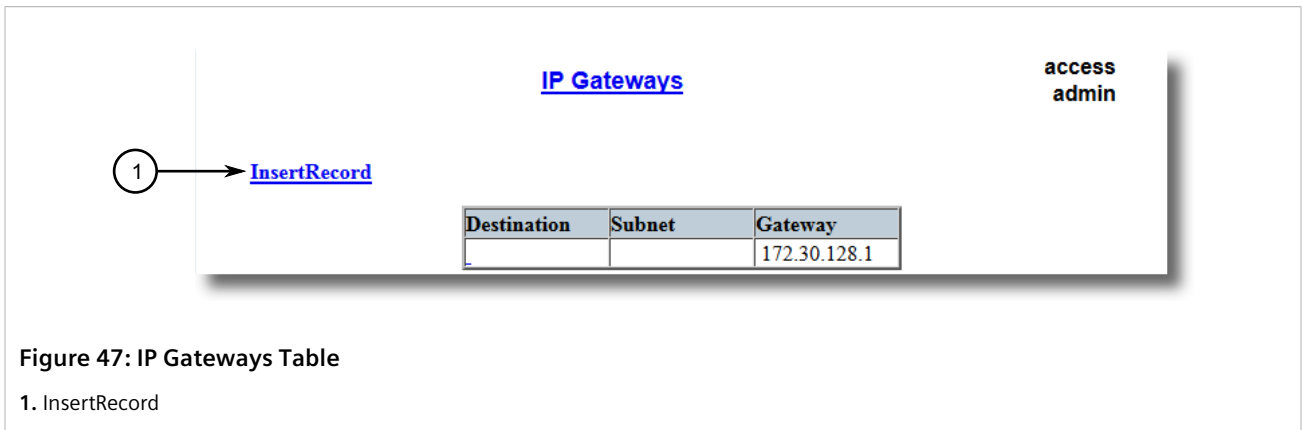
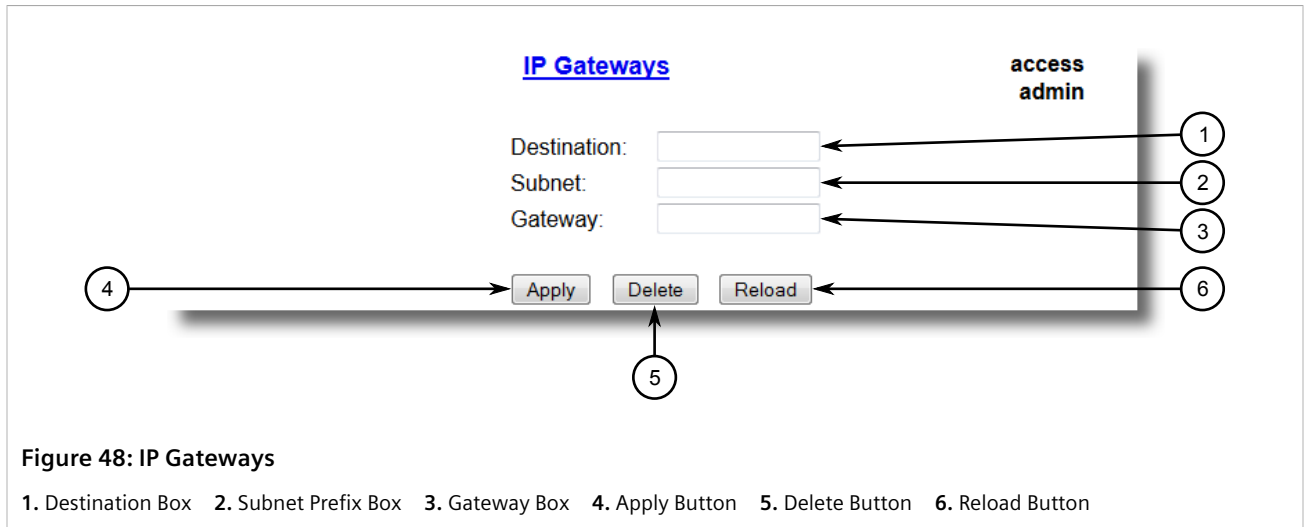


Figure 47: IP Gateways Table

1. InsertRecord

2. Click **InsertRecord**. The **IP Gateways** form appears.



3. Configure the following parameter(s) as required:

Parameter	Description
Destination	<b>Synopsis:</b> ###.###.###.### where ### ranges from 0 to 255 Specifies the IP address of destination network or host. For default gateway, both the destination and subnet are 0.
Subnet	<b>Synopsis:</b> ###.###.###.### where ### ranges from 0 to 255 Specifies the destination IP subnet mask. For default gateway, both the destination and subnet are 0.
Gateway	<b>Synopsis:</b> ###.###.###.### where ### ranges from 0 to 255 Specifies the gateway to be used to reach the destination.

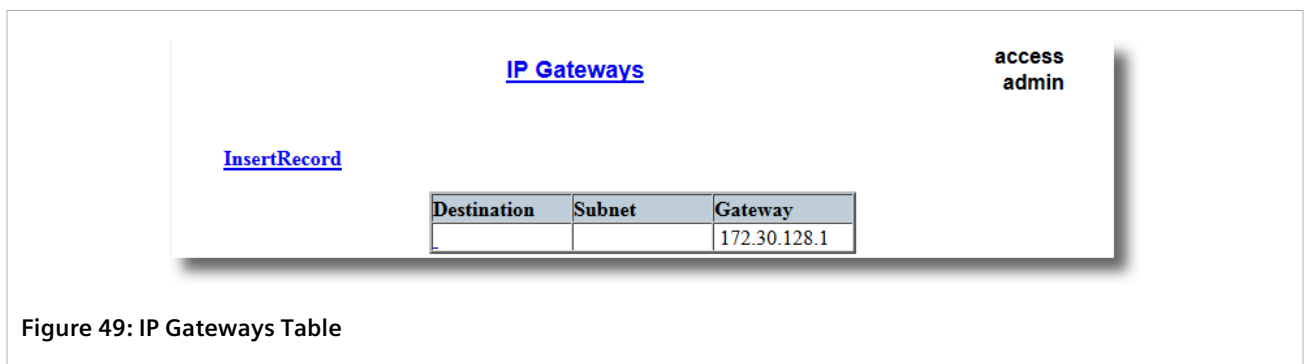
4. Click **Apply**.

Section 4.8.3

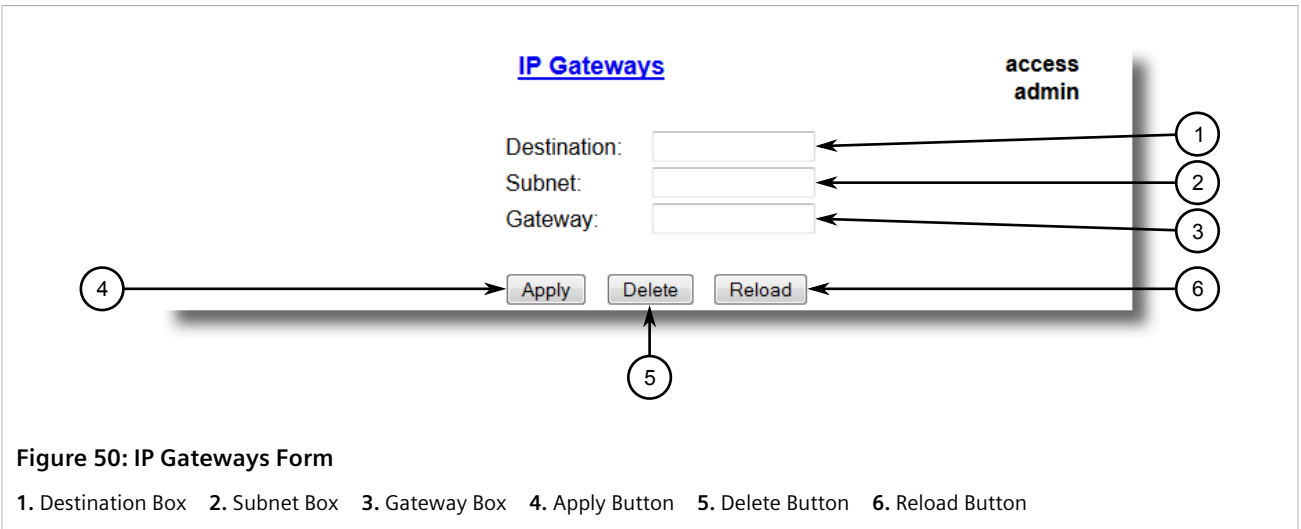
## Deleting an IP Gateway

To delete an IP gateway configured on the device, do the following:

1. Navigate to **Administration » Configure IP Gateways**. The **IP Gateways** table appears.



2. Select the IP gateway from the table. The **IP Gateways** form appears.



3. Click **Delete**.

Section 4.9

## Configuring DNS Servers

RUGGEDCOM ROS can be configured to use two DNS servers: a primary server and a backup server. If the primary server is unavailable, the device will automatically attempt to connect with the backup server.

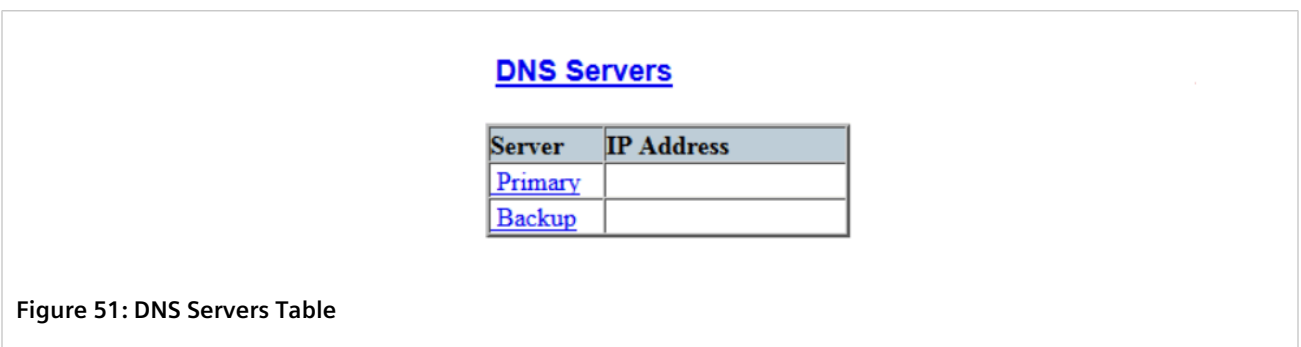


**IMPORTANT!**

*DHCP-provided DNS servers will override manually configured values.*

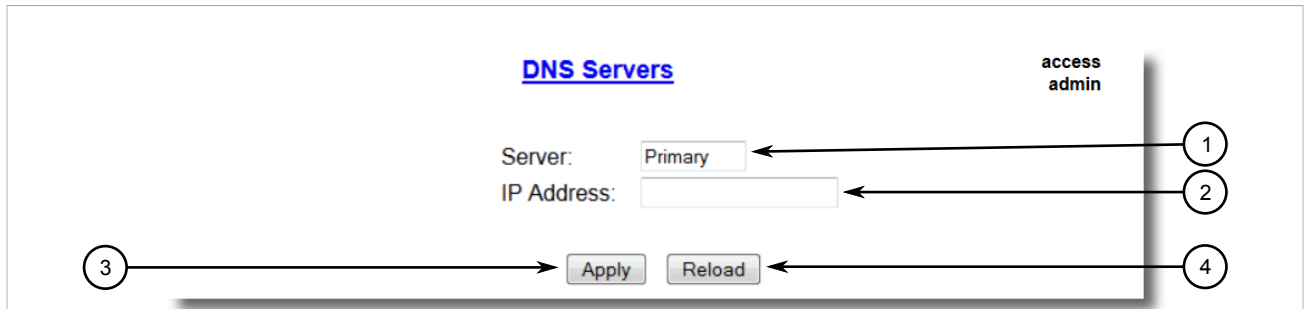
To configure access to either the primary or backup DNS servers, do the following

1. Navigate to **Administration » Configure DNS Servers**. The **DNS Servers** form appears.



2. Select either **Primary** or **Backup** from the table. The **DNS Server** form appears.





**Figure 52: DNS Server Form**

1. Server Box 2. IP Address Box 3. Apply Button 4. Reload Button

3. Configure the following parameter(s) as required:

Parameter	Description
Server	<b>Synopsis:</b> Any 8 characters <b>Default:</b> Primary This field tells whether this configuration is for a Primary or a Backup Server.
IP Address	<b>Synopsis:</b> ###.###.###.### where ### ranges from 0 to 255 The Server IP Address.

4. Click **Apply**.

Section 4.10

## Configuring IP Services

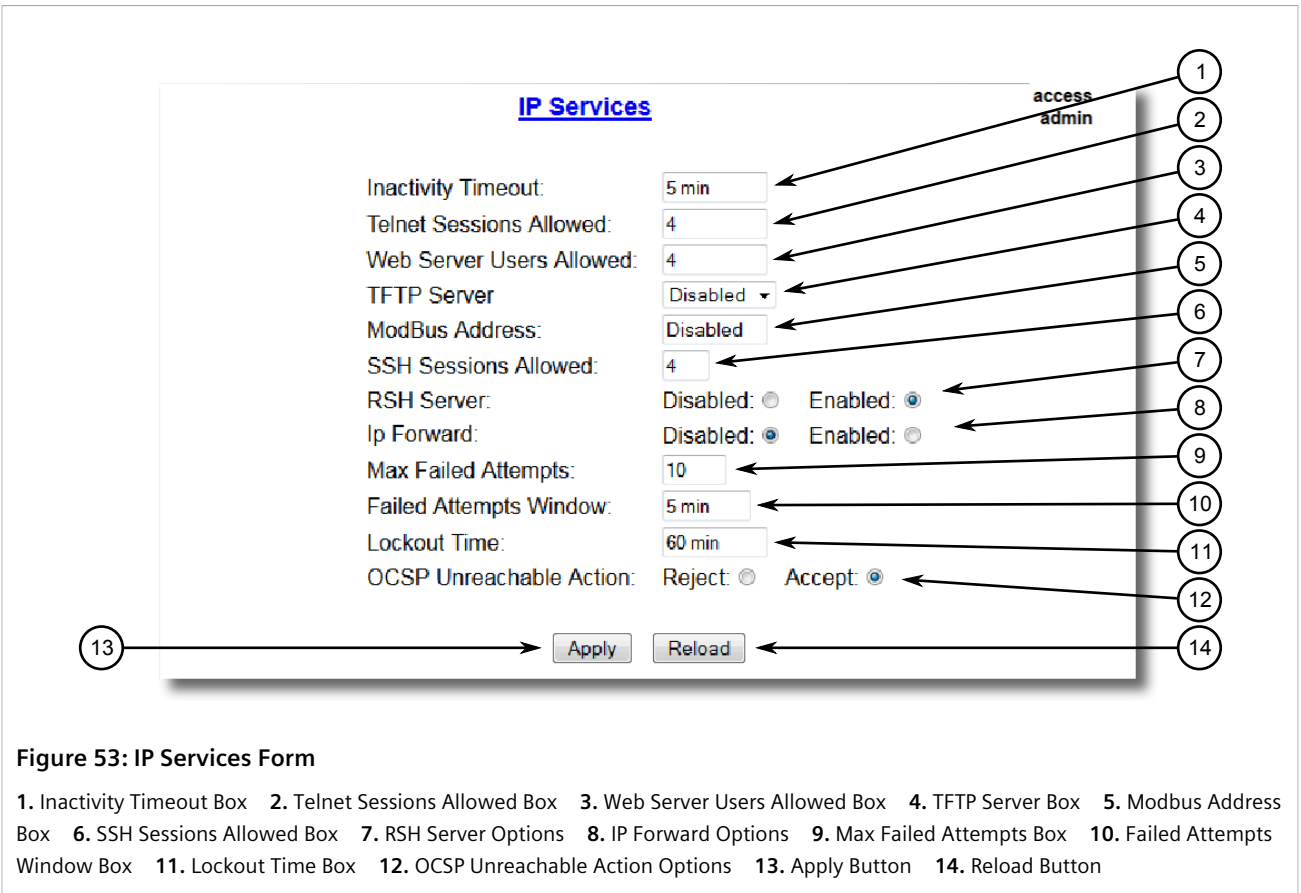
To configure the IP services provided by the device, do the following:



**IMPORTANT!**

*The following insecure protocols are disabled by default in RUGGEDCOM ROS: RSH, Telnet, TFTP, and ModBus management. To meet varied customer needs, these protocols can be enabled, but enabling them will break compliance with FIPS 140-2. For more information, refer to the **FIPS 140-2 Non-Proprietary Security Policy** or contact Siemens Customer Support.*

1. Navigate to **Administration » Configure IP Services**. The **IP Services** form appears.




**Figure 53: IP Services Form**

1. Inactivity Timeout Box 2. Telnet Sessions Allowed Box 3. Web Server Users Allowed Box 4. TFTP Server Box 5. Modbus Address Box 6. SSH Sessions Allowed Box 7. RSH Server Options 8. IP Forward Options 9. Max Failed Attempts Box 10. Failed Attempts Window Box 11. Lockout Time Box 12. OCSP Unreachable Action Options 13. Apply Button 14. Reload Button

2. Configure the following parameter(s) as required:

Parameter	Description
Inactivity Timeout	<b>Synopsis:</b> 1 to 60 or { Disabled } <b>Default:</b> 5 min Specifies when the console will timeout and display the login screen if there is no user activity. A value of zero disables timeouts. For Web Server users maximum timeout value is limited to 30 minutes.
Telnet Sessions Allowed	<b>Synopsis:</b> 1 to 4 or { Disabled } <b>Default:</b> Disabled Limits the number of Telnet sessions. A value of zero prevents any Telnet access.
Web Server Users Allowed	<b>Synopsis:</b> 1 to 4 or { Disabled } <b>Default:</b> 4 Limits the number of simultaneous web server users.
TFTP Server	<b>Synopsis:</b> { Disabled, Get Only, Enabled } <b>Default:</b> Disabled As TFTP is a very insecure protocol, this parameter allows user to limit or disable TFTP Server access.. DISABLED - disables read and write access to TFTP Server GET ONLY - only allows reading of files via TFTP Server ENABLED - allows reading and writing of files via TFTP Server
ModBus Address	<b>Synopsis:</b> 1 to 255 or { Disabled } <b>Default:</b> Disabled

Parameter	Description
	Determines the Modbus address to be used for Management through Modbus.
SSH Sessions Allowed (Controlled Version Only)	<b>Synopsis:</b> 1 to 4 <b>Default:</b> 4 Limits the number of SSH sessions.
RSH Server	<b>Synopsis:</b> { Disabled, Enabled } <b>Default:</b> Disabled (controlled version) or Enabled (non-controlled version) Disables/enables Remote Shell access.
IP Forward	<b>Synopsis:</b> { Disabled, Enabled } Controls the ability of IP Forwarding between VLANs in Serial Server or IP segments.  <div style="border: 1px solid black; padding: 5px; background-color: #f0f0f0;">  <b>NOTE</b> When upgrading to ROS-F v4.2.2.F, the default will be set to { Enabled }.                 </div>
Max Failed Attempts	<b>Synopsis:</b> 1 to 20 <b>Default:</b> 10 Maximum number of consecutive failed access attempts on service within Failed Attempts Window before blocking the service.
Failed Attempts Window	<b>Synopsis:</b> 1 to 30 min <b>Default:</b> 5 min The time in minutes (min) in which the maximum number of failed login attempts must be exceeded before a service is blocked. The counter of failed attempts resets to 0 when the timer expires.
Lockout Time	<b>Synopsis:</b> 1 to 120 min <b>Default:</b> 60 min The time in minutes (min) the service remains locked out after the maximum number of failed access attempts has been reached.
OCSP Unreachable Action	<b>Synopsis:</b> { Reject, Accept } <b>Default:</b> Reject The action to take if OCSP server is unreachable.

3. Click **Apply**.

Section 4.11

## Managing Remote Monitoring

Remote Monitoring (RMON) is used to collect and view historical statistics related to the performance and operation of Ethernet ports. It can also record a log entry and/or generate an SNMP trap when the rate of occurrence of a specified event is exceeded.

### CONTENTS

- [Section 4.11.1, “Managing RMON History Controls”](#)
- [Section 4.11.2, “Managing RMON Alarms”](#)
- [Section 4.11.3, “Managing RMON Events”](#)

Section 4.11.1

## Managing RMON History Controls

The history controls for Remote Monitoring take samples of the RMON-MIB history statistics of an Ethernet port at regular intervals.

### CONTENTS

- [Section 4.11.1.1, “Viewing a List of RMON History Controls”](#)
- [Section 4.11.1.2, “Adding an RMON History Control”](#)
- [Section 4.11.1.3, “Deleting an RMON History Control”](#)

Section 4.11.1.1

### Viewing a List of RMON History Controls

To view a list of RMON history controls, navigate to *Ethernet Stats » Configure RMON History Controls*. The **RMON History Controls** table appears.

Index	Port	Requested Buckets	Granted Buckets	Interval	Owner
<a href="#">1</a>	1	50	50	2	Monitor

Figure 54: RMON History Controls Table

If history controls have not been configured, add controls as needed. For more information, refer to [Section 4.11.1.2, “Adding an RMON History Control”](#).

Section 4.11.1.2

### Adding an RMON History Control

To add an RMON history control, do the following:

1. Navigate to *Ethernet Stats » Configure RMON History Controls*. The **RMON History Controls** table appears.

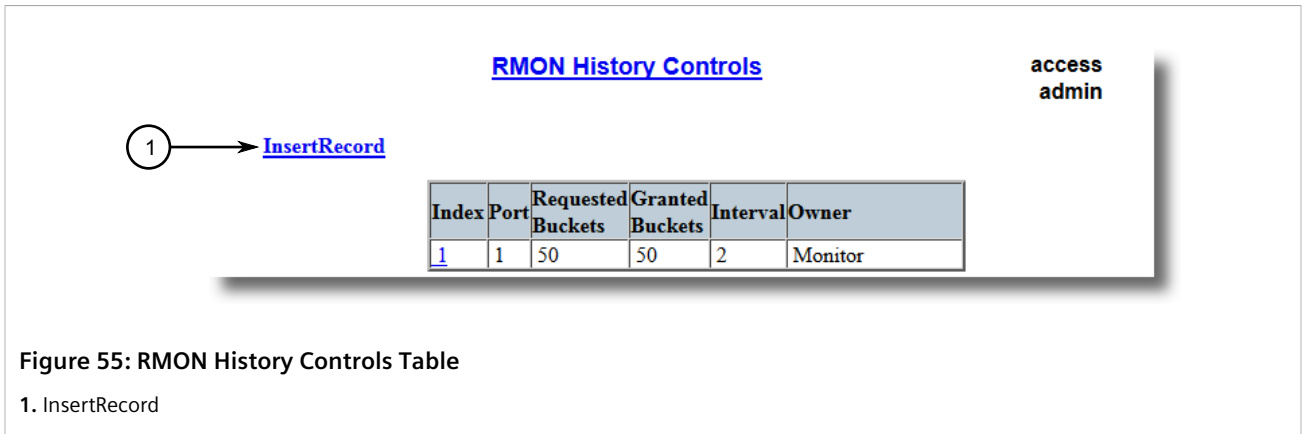


Figure 55: RMON History Controls Table

1. InsertRecord

- Click **InsertRecord**. The **RMON History Controls** form appears.

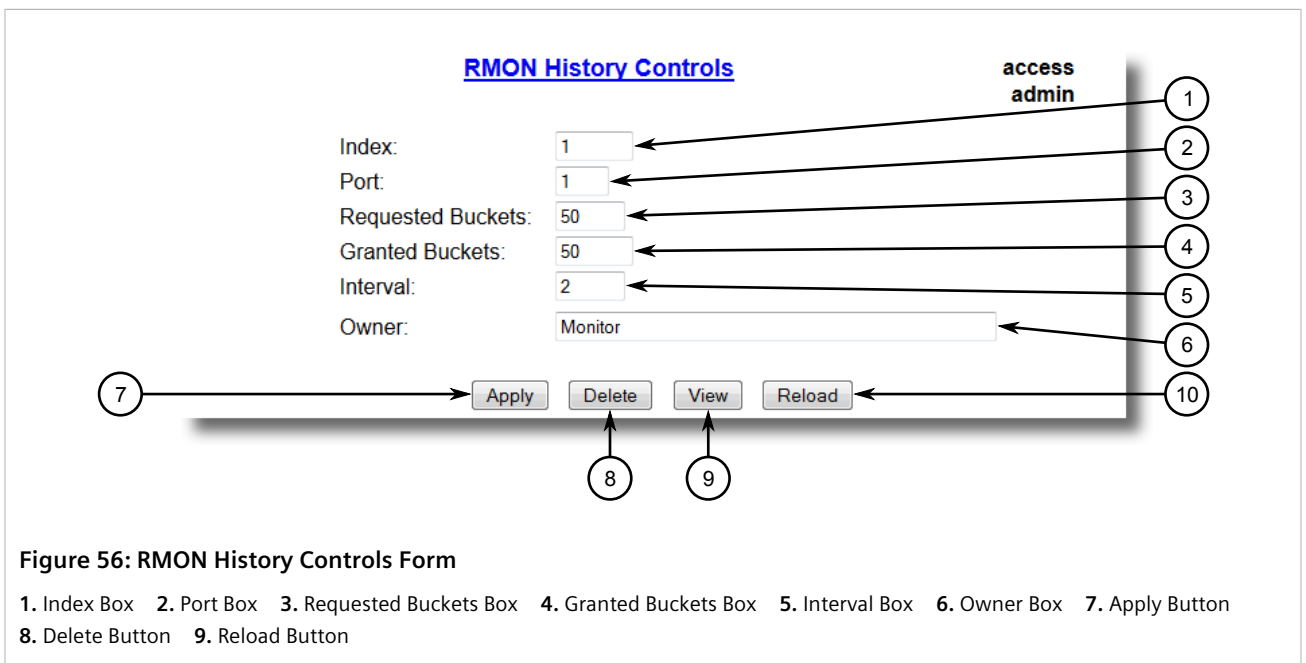


Figure 56: RMON History Controls Form

1. Index Box 2. Port Box 3. Requested Buckets Box 4. Granted Buckets Box 5. Interval Box 6. Owner Box 7. Apply Button  
8. Delete Button 9. Reload Button

- Configure the following parameter(s) as required:

Parameter	Description
Index	<b>Synopsis:</b> 1 to 65535 <b>Default:</b> 1 The index of this RMON History Control record.
Port	<b>Synopsis:</b> 1 to maximum port number <b>Default:</b> 1 The port number as seen on the front plate silkscreen of the switch.
Requested Buckets	<b>Synopsis:</b> 1 to 4000 <b>Default:</b> 50 The maximum number of buckets requested for this RMON collection history group of statistics. The range is 1 to 4000. The default is 50.
Granted Buckets	<b>Synopsis:</b> 0 to 65535

Parameter	Description
	The number of buckets granted for this RMON collection history. This field is not editable.
Interval	<b>Synopsis:</b> 1 to 3600 <b>Default:</b> 1800 The number of seconds in over which the data is sampled for each bucket. The range is 1 to 3600. The default is 1800.
Owner	<b>Synopsis:</b> Any 127 characters <b>Default:</b> Monitor The owner of this record. It is suggested to start this string with word 'monitor'.

4. Click **Apply**.

Section 4.11.1.3

## Deleting an RMON History Control

To delete an RMON history control, do the following:

1. Navigate to **Ethernet Stats » Configure RMON History Controls**. The **RMON History Controls** table appears.

[RMON History Controls](#)

access  
admin

[InsertRecord](#)

Index	Port	Requested Buckets	Granted Buckets	Interval	Owner
<a href="#">1</a>	1	50	50	2	Monitor

**Figure 57: RMON History Controls Table**

2. Select the history control from the table. The **RMON History Controls** form appears.

The screenshot shows the 'RMON History Controls' form. It includes the following fields and buttons:

- Index: 1
- Port: 1
- Requested Buckets: 50
- Granted Buckets: 50
- Interval: 2
- Owner: Monitor
- Buttons: Apply, Delete, View, Reload

Numbered callouts (1-10) point to the following elements:

- Index input box
- Port input box
- Requested Buckets input box
- Granted Buckets input box
- Interval input box
- Owner input box
- Apply button
- Delete button
- Reload button
- View button

**Figure 58: RMON History Controls Form**

1. Index Box 2. Port Box 3. Requested Buckets Box 4. Granted Buckets Box 5. Interval Box 6. Owner Box 7. Apply Button  
8. Delete Button 9. Reload Button

3. Click **Delete**.

#### Section 4.11.2

## Managing RMON Alarms

When Remote Monitoring (RMON) alarms are configured, RUGGEDCOM ROS examines the state of a specific statistical variable.

Remote Monitoring (RMON) alarms define upper and lower thresholds for legal values of specific statistical variables in a given interval. This allows RUGGEDCOM ROS to detect events as they occur more quickly than a specified maximum rate or less quickly than a minimum rate.

When the rate of change for a statistics value exceeds its limits, an internal INFO alarm is always generated. For information about viewing alarms, refer to [Section 5.4.2, "Viewing and Clearing Latched Alarms"](#).

Additionally, a statistic threshold crossing can result in further activity. An RMON alarm can be configured to point to a particular RMON event, which can generate an SNMP trap, an entry in the event log, or both. The RMON event can also direct alarms towards different users defined for SNMP.

The alarm can point to a different event for each of the thresholds. Therefore, combinations such as *trap on rising threshold* or *trap on rising threshold, log and trap on falling threshold* are possible.

Each RMON alarm may be configured such that its first instance occurs only for rising, falling, or all thresholds that exceed their limits.

The ability to configure upper and lower thresholds on the value of a measured statistic provides for the ability to add hysteresis to the alarm generation process.

If the value of the measured statistic over time is compared to a single threshold, alarms will be generated each time the statistic crosses the threshold. If the statistic's value fluctuates around the threshold, an alarm can be generated every measurement period. Programming different upper and lower thresholds eliminates spurious alarms. The statistic value must *travel* between the thresholds before alarms can be generated. The following illustrates the very different patterns of alarm generation resulting from a statistic sample and the same sample with hysteresis applied.

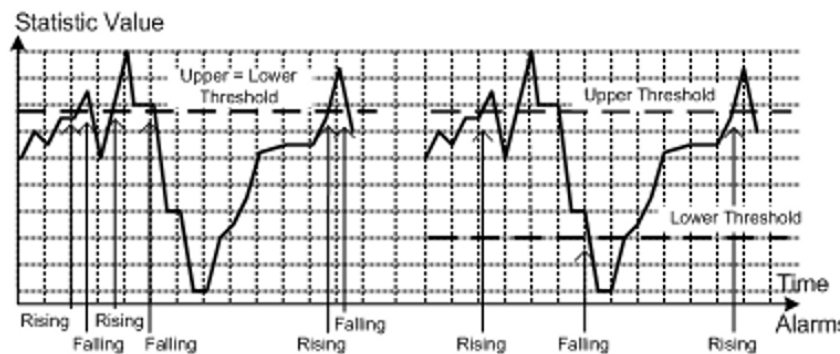


Figure 59: The Alarm Process

There are two methods to evaluate a statistic to determine when to generate an event: delta and absolute.

For most statistics, such as line errors, it is appropriate to generate an alarm when a rate is exceeded. The alarm defaults to the *delta* measurement method, which examines changes in a statistic at the end of each measurement period.

It may be desirable to alarm when the total, or absolute, number of events crosses a threshold. In this case, set the measurement period type to *absolute*.

#### CONTENTS

- [Section 4.11.2.1, "Viewing a List of RMON Alarms"](#)
- [Section 4.11.2.2, "Adding an RMON Alarm"](#)
- [Section 4.11.2.3, "Deleting an RMON Alarm"](#)

#### Section 4.11.2.1

### Viewing a List of RMON Alarms

To view a list of RMON alarms, navigate to **Ethernet Stats » Configure RMON Alarms**. The **RMON Alarms** table appears.

<a href="#">RMON Alarms</a>							access admin
<a href="#">InsertRecord</a>							
Index	Variable	Rising Thr	Falling Thr	Value	Type	Interval	Start
<a href="#">1</a>	ifInOctets.1	150	100	0	delta	1	rising

Figure 60: RMON Alarms Table

If alarms have not been configured, add alarms as needed. For more information, refer to [Section 4.11.2.2, "Adding an RMON Alarm"](#).

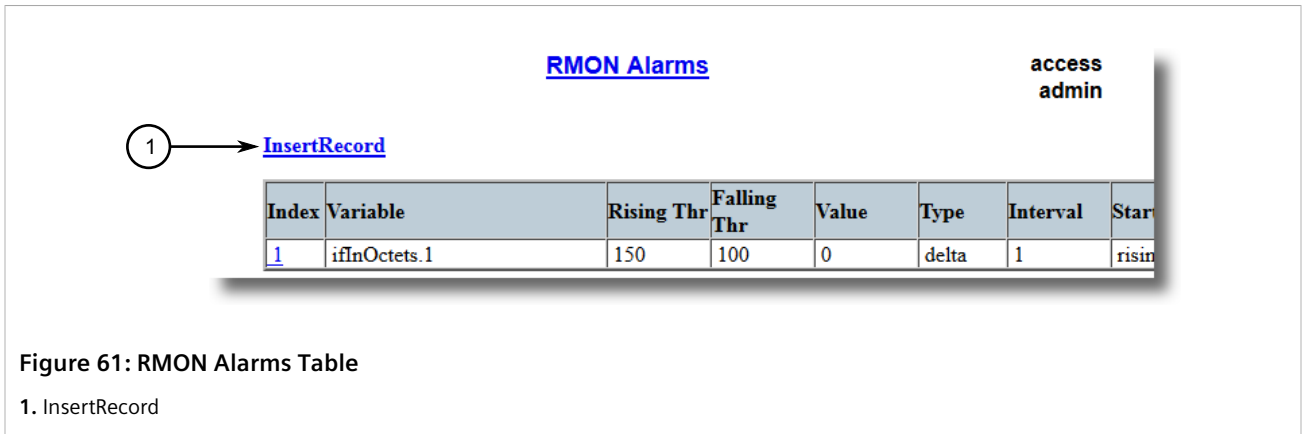


Section 4.11.2.2

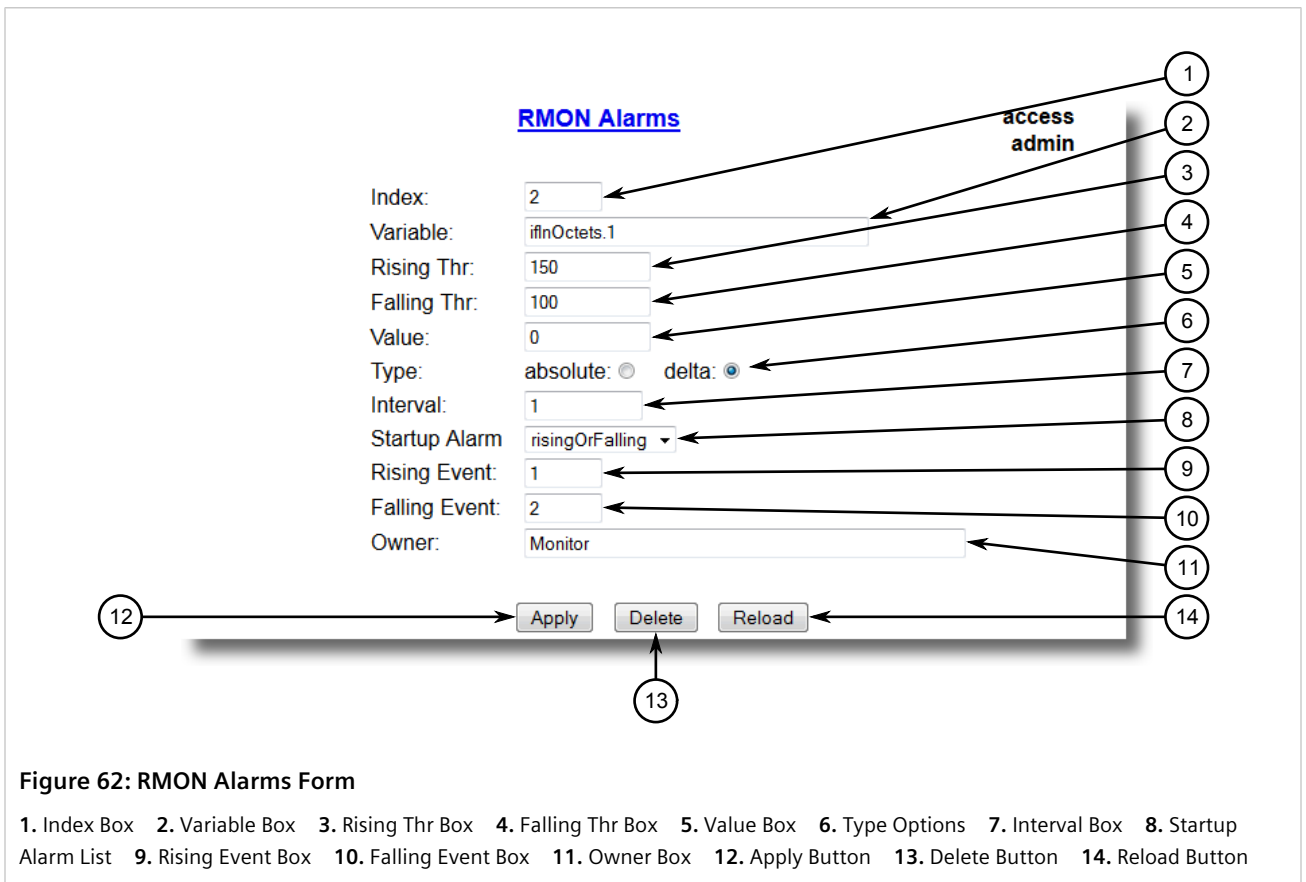
## Adding an RMON Alarm

To add an RMON alarm, do the following:

1. Navigate to **Ethernet Stats » Configure RMON Alarms**. The **RMON Alarms** table appears.



2. Click **InsertRecord**. The **RMON Alarms** form appears.



3. Configure the following parameter(s) as required:

Parameter	Description
Index	Synopsis: 1 to 65535

Parameter	Description
	<b>Default:</b> 1 The index of this RMON Alarm record.
Variable	<b>Synopsis:</b> SNMP Object Identifier - up to 39 characters The SNMP object identifier (OID) of the particular variable to be sampled. Only variables that resolve to an ASN.1 primitive type INTEGER (INTEGER, Integer32, Counter32, Counter64, Gauge, or TimeTicks) may be sampled. A list of objects can be printed using shell command 'rmon'. The OID format: objectName.index1.index2... where index format depends on index object type.
Rising Thr	<b>Synopsis:</b> -2147483647 to 2147483647 <b>Default:</b> 0 A threshold for the sampled variable. When the current sampled variable value is greater than or equal to this threshold, and the value at the last sampling interval was less than this threshold, a single event will be generated. A single event will also be generated if the first sample after this record is created is greater than or equal to this threshold and the associated startup alarm is equal to 'rising'. After rising alarm is generated, another such event will not be generated until the sampled value falls below this threshold and reaches the value of FallingThreshold.
Falling Thr	<b>Synopsis:</b> -2147483647 to 2147483647 <b>Default:</b> 0 A threshold for the sampled variable. When the current sampled variable value is less than or equal to this threshold, and the value at the last sampling interval was greater than this threshold, a single event will be generated. A single event will also be generated if the first sample after this record is created is less than or equal to this threshold and the associated startup alarm is equal to 'falling'. After falling alarm is generated, another such event will not be generated until the sampled value rises above this threshold and reaches the value of RisingThreshold.
Value	<b>Synopsis:</b> -2147483647 to 2147483647 The value of monitoring object during the last sampling period. The presentation of value depends of sample type ('absolute' or 'delta').
Type	<b>Synopsis:</b> { absolute, delta } <b>Default:</b> delta The method of sampling the selected variable and calculating the value to be compared against the thresholds. The value of sample type can be 'absolute' or 'delta'.
Interval	<b>Synopsis:</b> 0 to 2147483647 <b>Default:</b> 60 The number of seconds in over which the data is sampled and compared with the rising and falling thresholds.
Startup Alarm	<b>Synopsis:</b> { rising, falling, risingOrFalling } <b>Default:</b> risingOrFalling The alarm that may be sent when this record is first created if condition for raising alarm is met. The value of startup alarm can be 'rising', 'falling' or 'risingOrFalling'.
Rising Event	<b>Synopsis:</b> 0 to 65535 <b>Default:</b> 0 The index of the event that is used when a falling threshold is crossed. If there is no corresponding entry in the Event Table, then no association exists. In particular, if this value is zero, no associated event will be generated.
Falling Event	<b>Synopsis:</b> 0 to 65535 <b>Default:</b> 0 The index of the event that is used when a rising threshold is crossed. If there is no corresponding entry in the Event Table, then no association exists. In particular, if this value is zero, no associated event will be generated.
Owner	<b>Synopsis:</b> Any 127 characters

Parameter	Description
	<p><b>Default:</b> Monitor</p> <p>The owner of this record. It is suggested to start this string with word 'monitor'.</p>

- Click **Apply**.

Section 4.11.2.3

## Deleting an RMON Alarm

To delete an RMON alarm, do the following:

- Navigate to **Ethernet Stats » Configure RMON Alarms**. The **RMON Alarms** table appears.

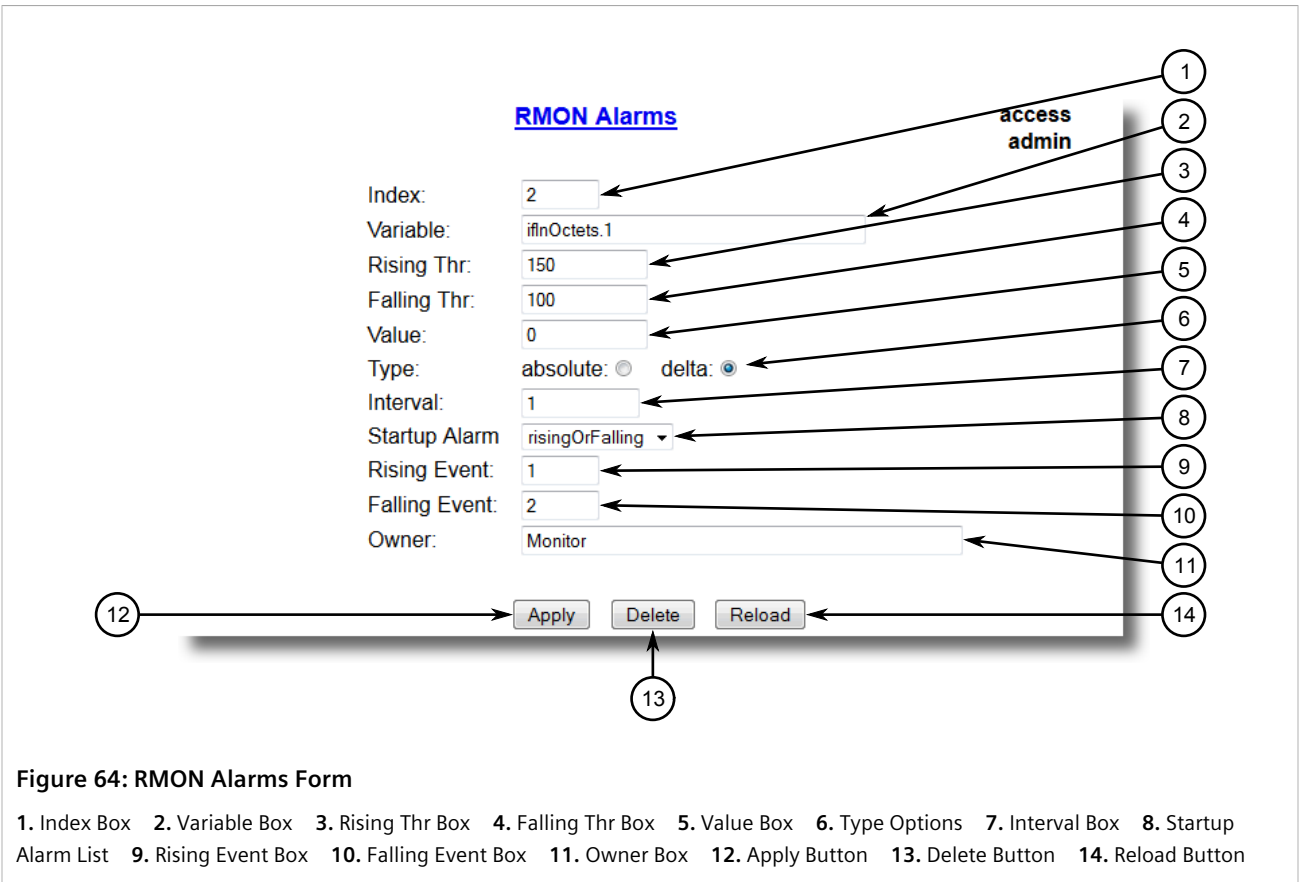
[RMON Alarms](#) access admin

[InsertRecord](#)

Index	Variable	Rising Thr	Falling Thr	Value	Type	Interval	Start
<a href="#">1</a>	ifInOctets.1	150	100	0	delta	1	rising

**Figure 63: RMON Alarms Table**

- Select the alarm from the table. The **RMON Alarms** form appears.



3. Click **Delete**.

### Section 4.11.3

## Managing RMON Events

Remote Monitoring (RMON) events define behavior profiles used in event logging. These profiles are used by RMON alarms to send traps and log events.

Each alarm may specify that a log entry be created on its behalf whenever the event occurs. Each entry may also specify that a notification should occur by way of SNMP trap messages. In this case, the user for the trap message is specified as the *Community*.

Two traps are defined: risingAlarm and fallingAlarm.

### CONTENTS

- [Section 4.11.3.1, "Viewing a List of RMON Events"](#)
- [Section 4.11.3.2, "Adding an RMON Event"](#)
- [Section 4.11.3.3, "Deleting an RMON Event"](#)

Section 4.11.3.1

## Viewing a List of RMON Events

To view a list of RMON events, navigate to *Ethernet Stats » Configure RMON Events*. The **RMON Events** table appears.

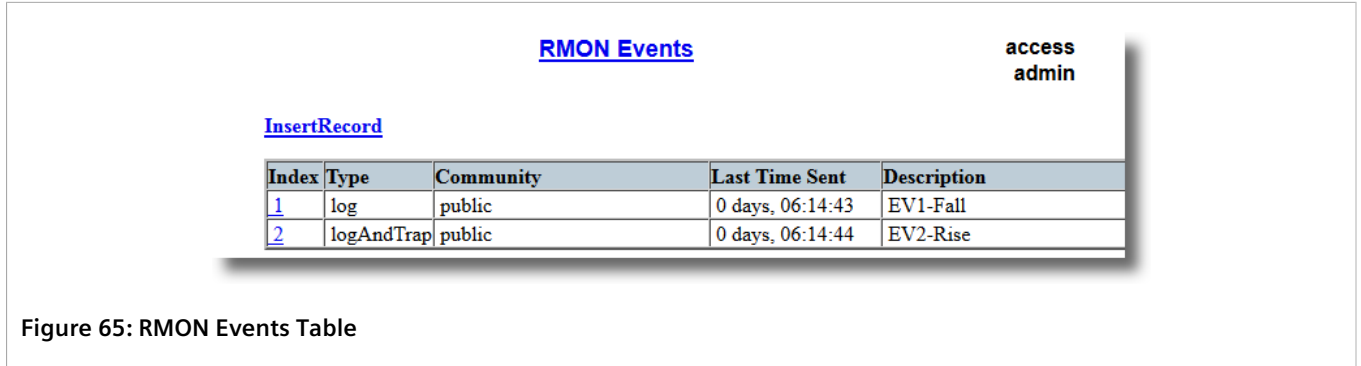


Figure 65: RMON Events Table

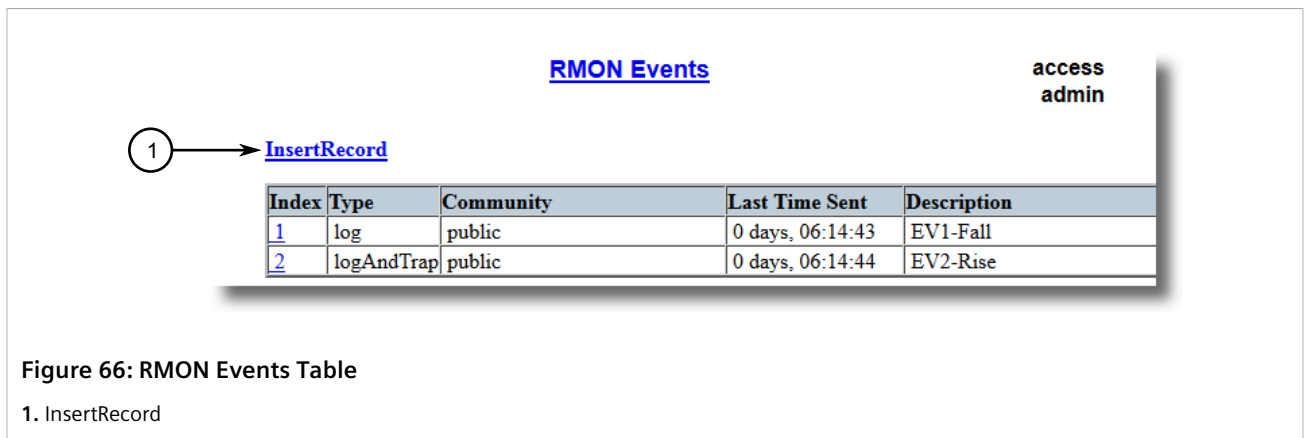
If events have not been configured, add events as needed. For more information, refer to [Section 4.11.3.2, "Adding an RMON Event"](#).

Section 4.11.3.2

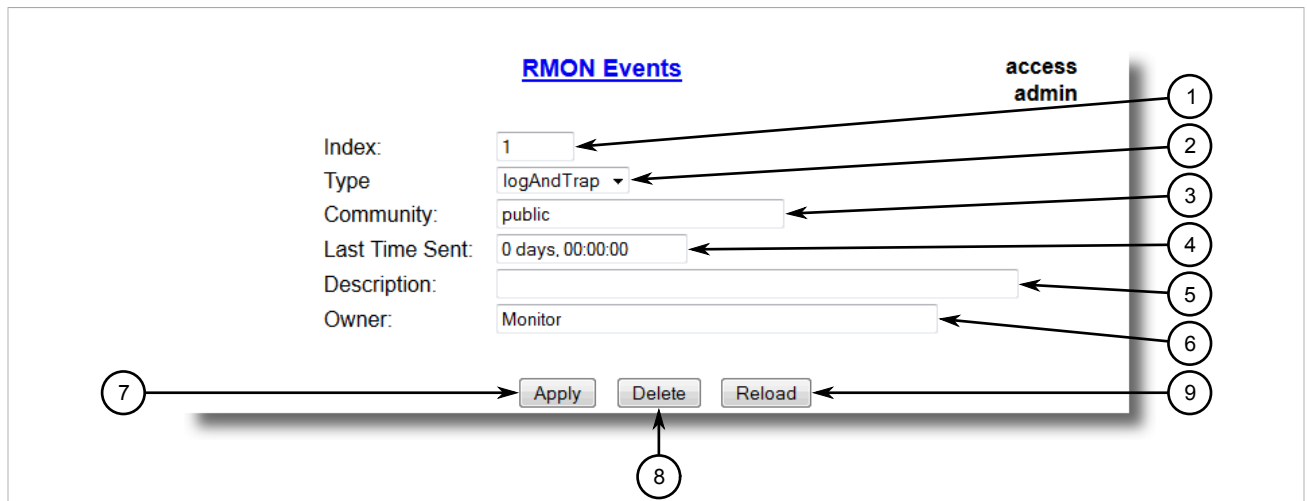
## Adding an RMON Event

To add an RMON alarm, do the following:

1. Navigate to *Ethernet Stats » Configure RMON Events*. The **RMON Events** table appears.



2. Click **InsertRecord**. The **RMON Events** form appears.



**Figure 67: RMON Events Form**

1. Index Box 2. Type List 3. Community Box 4. Last Time Sent Box 5. Description Box 6. Owner Box 7. Apply Button  
8. Delete Button 9. View Button 10. Reload Button

3. Configure the following parameter(s) as required:

Parameter	Description
Index	<b>Synopsis:</b> 1 to 65535 <b>Default:</b> 3 The index of this RMON Event record.
Type	<b>Synopsis:</b> { none, log, snmpTrap, logAndTrap } <b>Default:</b> logAndTrap The type of notification that the probe will make about this event. In the case of 'log', an entry is made in the RMON Log table for each event. In the case of snmp_trap, an SNMP trap is sent to one or more management stations.
Community	<b>Synopsis:</b> Any 31 characters <b>Default:</b> public If the SNMP trap is to be sent, it will be sent to the SNMP community specified by this string.
Last Time Sent	<b>Synopsis:</b> DDDD days, HH:MM:SS The time from last reboot at the time this event entry last generated an event. If this entry has not generated any events, this value will be 0.
Description	<b>Synopsis:</b> Any 127 characters <b>Default:</b> EV2-Rise A comment describing this event.
Owner	<b>Synopsis:</b> Any 127 characters <b>Default:</b> Monitor The owner of this event record. It is suggested to start this string with word 'monitor'.

4. Click **Apply**.

Section 4.11.3.3

## Deleting an RMON Event

To delete an RMON event, do the following:

1. Navigate to **Ethernet Stats » Configure RMON Events**. The RMON Events table appears.

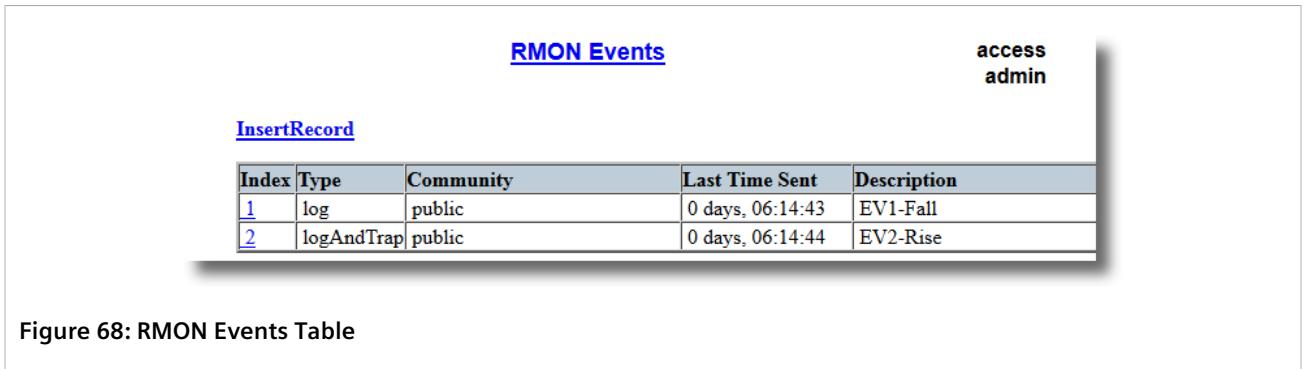


Figure 68: RMON Events Table

2. Select the event from the table. The RMON Events form appears.

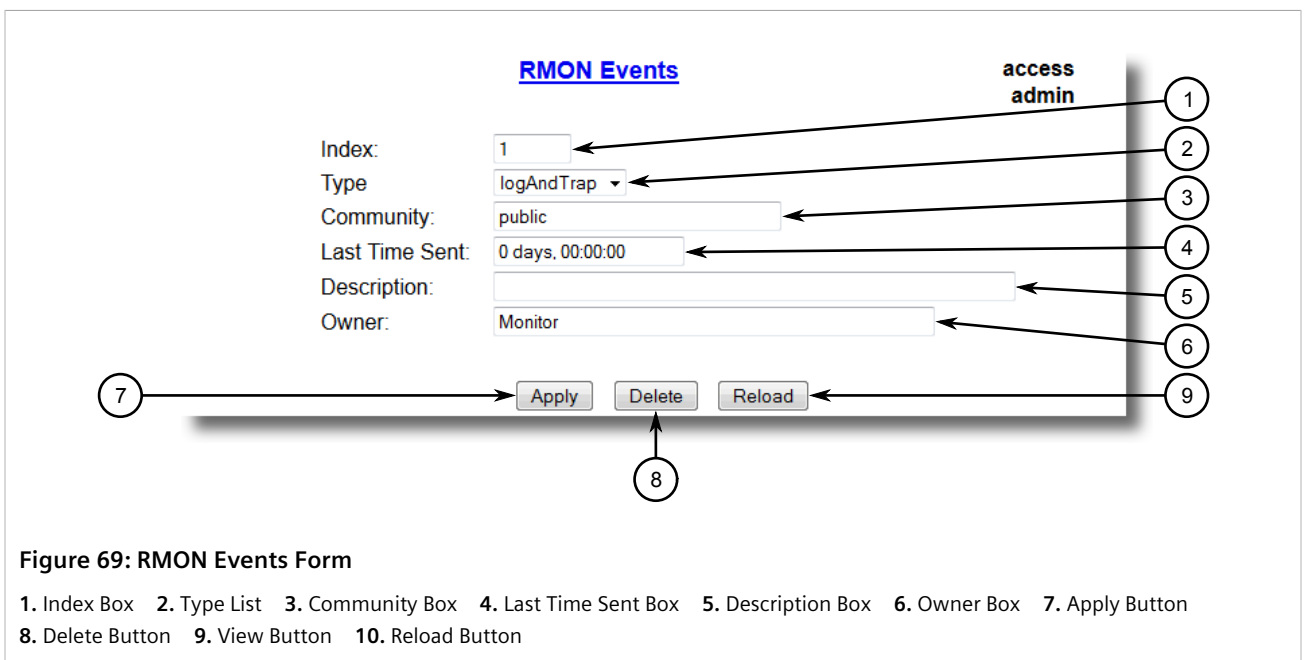


Figure 69: RMON Events Form

1. Index Box 2. Type List 3. Community Box 4. Last Time Sent Box 5. Description Box 6. Owner Box 7. Apply Button  
8. Delete Button 9. View Button 10. Reload Button

3. Click **Delete**.

Section 4.12

## Upgrading/Downgrading Firmware

This section describes how to upgrade and downgrade the firmware for RUGGEDCOM ROS.

### CONTENTS

- [Section 4.12.1, "Upgrading Firmware"](#)

- [Section 4.12.2, “Downgrading Firmware”](#)

### Section 4.12.1

## Upgrading Firmware

Upgrading RUGGEDCOM ROS firmware, including the main and FPGA firmware, may be necessary to take advantage of new features or bug fixes. Binary firmware releases, including updates, can be obtained by submitting a Support Request via the [Siemens Industry Online Support](https://support.industry.siemens.com) [https://support.industry.siemens.com] website. For more information, refer to <https://support.industry.siemens.com/My/ww/en/requests>.

Binary firmware images transferred to the device are stored in non-volatile Flash memory and require a device reset to take effect.



#### IMPORTANT!

*RUGGEDCOM ROS devices only accept new firmware digitally-signed by Siemens.*



#### NOTE

*The IP address set for the device will not be changed following a firmware upgrade.*

To upgrade the RUGGEDCOM ROS firmware, do the following:

1. Upload a different version of the binary firmware image to the device. For more information, refer to [Section 4.4, “Uploading/Downloading Files”](#).
2. Reset the device to complete the installation. For more information, refer to [Section 4.13, “Resetting the Device”](#).
3. Access the CLI shell and verify the new software version has been installed by typing **version**. The currently installed versions of the main and boot firmware are displayed.

```
>version  
Current ROS-CF52 Main Software v4.2.2.F.0 (Jan 01 4.2.2.F 00:01)
```

### Section 4.12.2

## Downgrading Firmware

Downgrading the RUGGEDCOM ROS firmware is generally not recommended, as it may have unpredictable effects. However, if a downgrade is required, do the following:



#### IMPORTANT!

*Before downgrading the firmware, make sure the hardware and FPGA code types installed in the device are supported by the older firmware version. Refer to the Release Notes for the older firmware version to confirm.*

1. Disconnect the device from the network.
2. Log in to the device as an admin user. For more information, refer to [Section 2.1, “Logging In”](#).
3. Make a local copy of the current configuration file. For more information, refer to [Section 4.4, “Uploading/Downloading Files”](#).



**!** **IMPORTANT!** *Never downgrade the firmware with encryption enabled to a version that does not support encryption.*

- Restore the device to its factory defaults. For more information, refer to [Section 4.3, “Restoring Factory Defaults”](#).
- Upload and apply the older firmware version and its associated FPGA files using the same methods used to install newer firmware versions. For more information, refer to [Section 4.12.1, “Upgrading Firmware”](#).
- Press **Ctrl-S** to access the CLI.
- Clear all logs by typing:

```
clearlogs
```

- Clear all alarms by typing:

```
clearalarms
```

**!** **IMPORTANT!** *After downgrading the firmware and FPGA files, be aware that some settings from the previous configuration may be lost or reverted back to the factory defaults (including user passwords if downgrading from a security related version), as those particular tables or fields may not exist in the older firmware version. Because of this, the unit must be configured after the downgrade.*

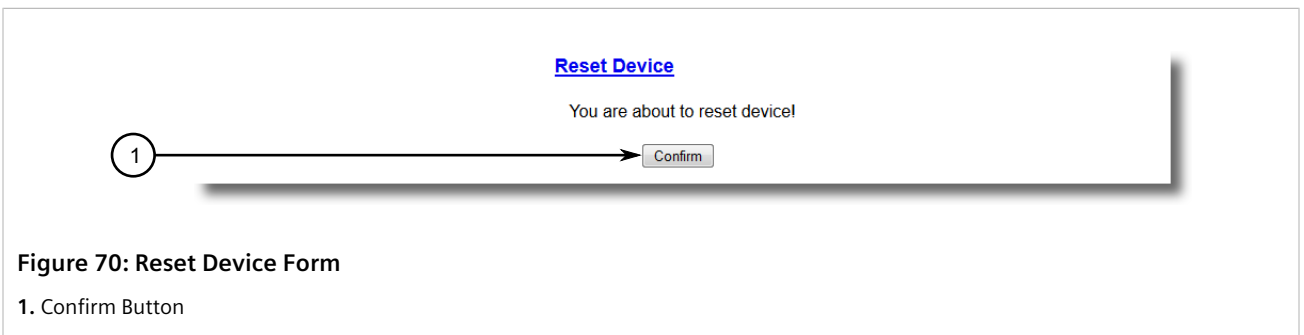
- Configure the device as required.

Section 4.13

# Resetting the Device

To reset the device, do the following:

- Navigate to **Diagnostics » Reset Device**. The **Reset Device** form appears.



- Click **Confirm**.

Section 4.14

## Clearing Data

Sometimes it may be necessary to permanently delete any sensitive, proprietary information. Before taking the device out of service, either permanently or for maintenance by a third-party, make sure the device has been fully decommissioned.

To clear data, do the following:

1. Disconnect all network cables from the device.
2. Connect to the device via the RS-232 serial console port. For more information, refer to [Section 3.1.2, "Connecting Directly"](#).
3. [Optional] Upload a blank version of the `banner.txt` file to the device to replace the existing file. For more information about uploading a file, refer to [Section 4.4, "Uploading/Downloading Files"](#).
4. [Optional] Confirm the upload was successful by typing:

```
type banner.txt
```

5. [Optional] Clear the local and system logs. For more information, refer to [Section 4.5.2, "Clearing Local and System Logs"](#).
6. Access maintenance mode. For more information, refer to [Section 2.8, "Accessing Maintenance Mode"](#). This will automatically delete the `ssl.crt`, `ssh.keys` and `config.csv` files.

# 5 System Administration

This chapter describes how to perform various administrative tasks related to device identification, user permissions, alarm configuration, certificates and keys, and more.

## CONTENTS

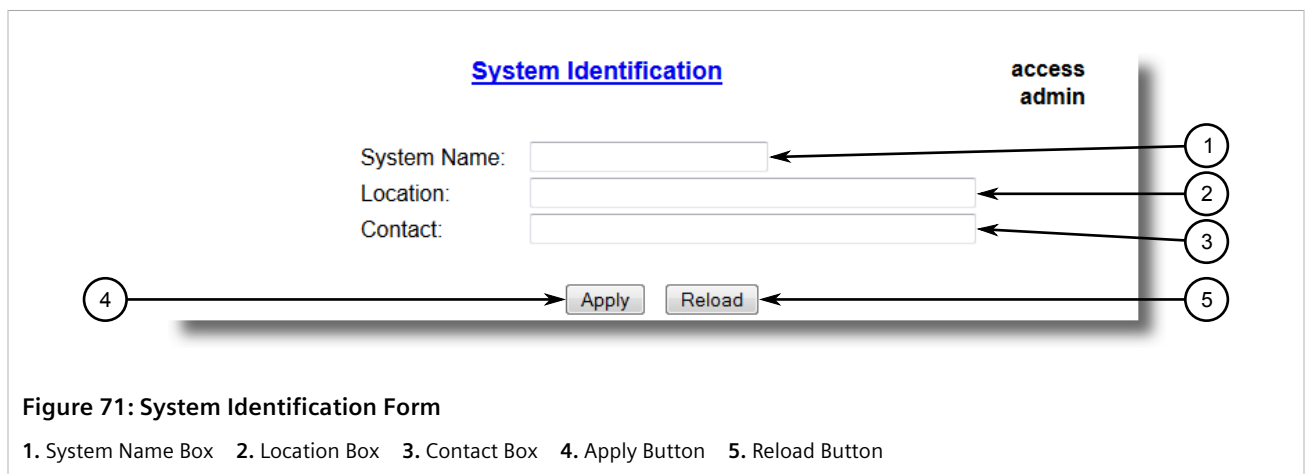
- [Section 5.1, "Configuring the System Information"](#)
- [Section 5.2, "Customizing the Login Screen"](#)
- [Section 5.3, "Enabling/Disabling the Web Interface"](#)
- [Section 5.4, "Managing Alarms"](#)
- [Section 5.5, "Managing the Configuration File"](#)

### Section 5.1

## Configuring the System Information

To configure basic information that can be used to identify the device, its location, and/or its owner, do the following:

1. Navigate to **Administration » Configure System Identification**. The **System Identification** form appears.



2. Configure the following parameter(s) as required:

Parameter	Description
System Name	<p><b>Synopsis:</b> Any 24 characters</p> <p>The system name is displayed in all RUGGEDCOM ROS menu screens. This can make it easier to identify the switches within your network provided that all switches are given a unique name.</p>

Parameter	Description
Location	<b>Synopsis:</b> Any 49 characters The location can be used to indicate the physical location of the switch. It is displayed in the login screen as another means to ensure you are dealing with the desired switch.
Contact	<b>Synopsis:</b> Any 49 characters The contact can be used to help identify the person responsible for managing the switch. You can enter name, phone number, email, etc. It is displayed in the login screen so that this person may be contacted should help be required.

3. Click **Apply**.

## Section 5.2

## Customizing the Login Screen

To display a custom welcome message, device information or any other information on the login screen for the Web and console interfaces, add text to the `banner.txt` file stored on the device.

**NOTE**

*If no banner text has been downloaded, a default banner will appear stating the following: "This device is for authorized users only. Disconnect IMMEDIATELY if you are not an authorized user!"*

To update the `banner.txt` file, download the file from the device, modify it and then load it back on to the device. For information about uploading and downloading files, refer to [Section 4.4, "Uploading/Downloading Files"](#).

## Section 5.3

## Enabling/Disabling the Web Interface

In some cases, users may want to disable the Web interface to increase cyber security.

To disable or enable the Web interface, do the following:

**NOTE**

*The Web interface can be disabled via the Web UI by configuring the Web Server Users Allowed parameter in the **IP Services form**. For more information, refer to [Section 4.10, "Configuring IP Services"](#).*

1. Log in to the device as an admin user and access the CLI shell. For more information about accessing the CLI shell, refer to [Section 2.5, "Using the Command Line Interface"](#).
2. Navigate to **Administration » Configure IP Services » Web Server Users Allowed**.
3. Select **Disabled** to disable the Web interface, or select the desired number of Web server users allowed to enable the interface.

## Section 5.4

# Managing Alarms

Alarms indicate the occurrence of events of either importance or interest that are logged by the device.

There are two types of alarms:

- **Active alarms** signify states of operation that are not in accordance with normal operation. Examples include links that should be up, but are not, or error rates that repeatedly exceed a certain threshold. These alarms are continuously active and are only cleared when the problem that triggered the alarms is resolved.
- **Passive alarms** are a record of abnormal conditions that occurred in the past and do not affect the current operation state of the device. Examples include authentication failures, Remote Network MONitoring (RMON) MIB generated alarms, or error states that temporarily exceeded a certain threshold. These alarms can be cleared from the list of alarms.

**NOTE**

For more information about RMON alarms, refer to [Section 4.11.2, "Managing RMON Alarms"](#).

When either type of alarm occurs, a message appears in the top right corner of the user interface. If more than one alarm has occurred, the message will indicate the number of alarms. Active alarms also trip the Critical Failure Relay LED on the device. The message and the LED will remain active until the alarm is cleared.

**NOTE**

Alarms are volatile in nature. All alarms (active and passive) are cleared at startup.

**CONTENTS**

- [Section 5.4.1, "Viewing a List of Pre-Configured Alarms"](#)
- [Section 5.4.2, "Viewing and Clearing Latched Alarms"](#)
- [Section 5.4.3, "Configuring an Alarm"](#)
- [Section 5.4.4, "Authentication Related Security Alarms"](#)

## Section 5.4.1

## Viewing a List of Pre-Configured Alarms

To view a list of alarms pre-configured for the device, navigate to **Diagnostic » Configure Alarms**. The **Alarms** table appears.

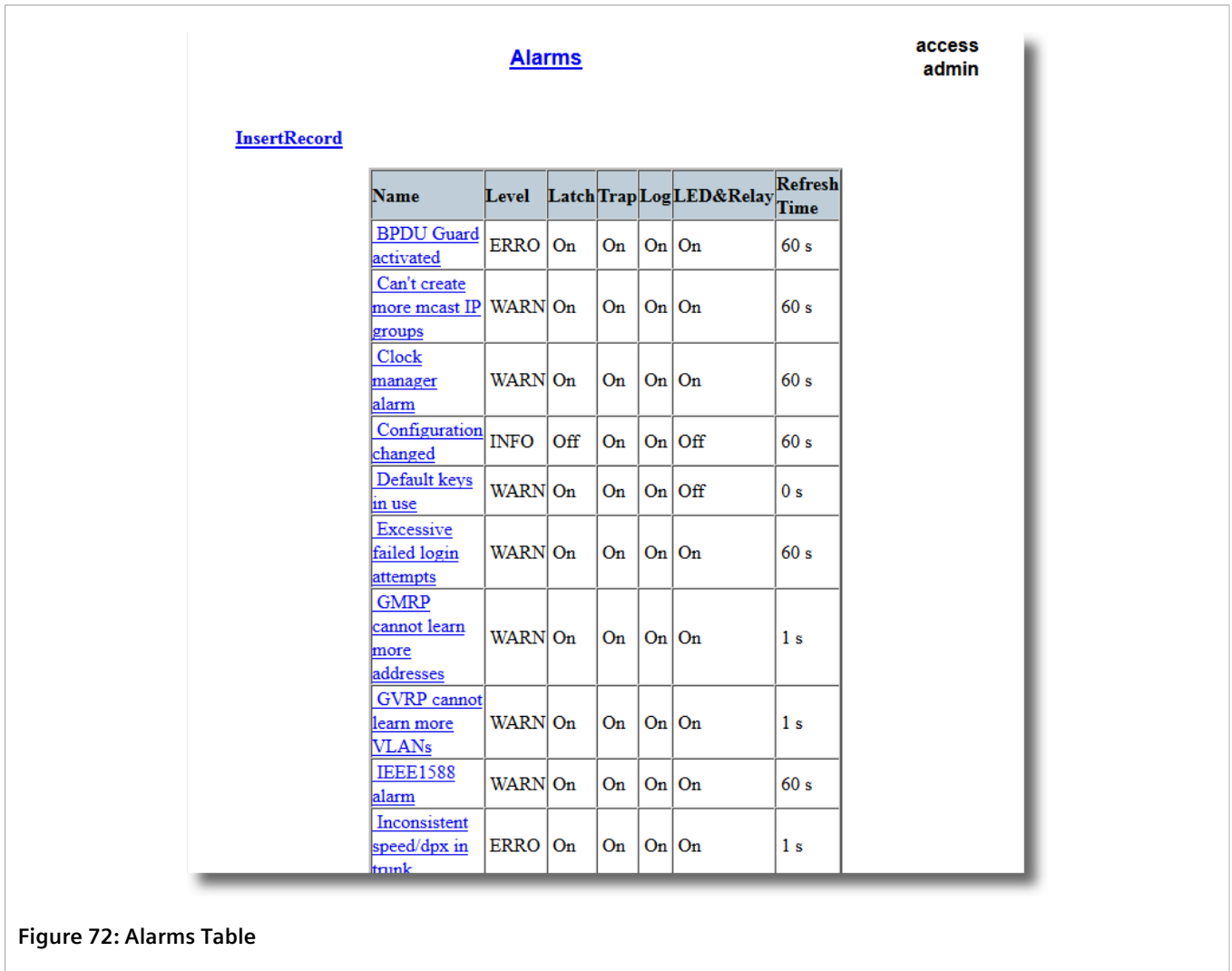



Figure 72: Alarms Table

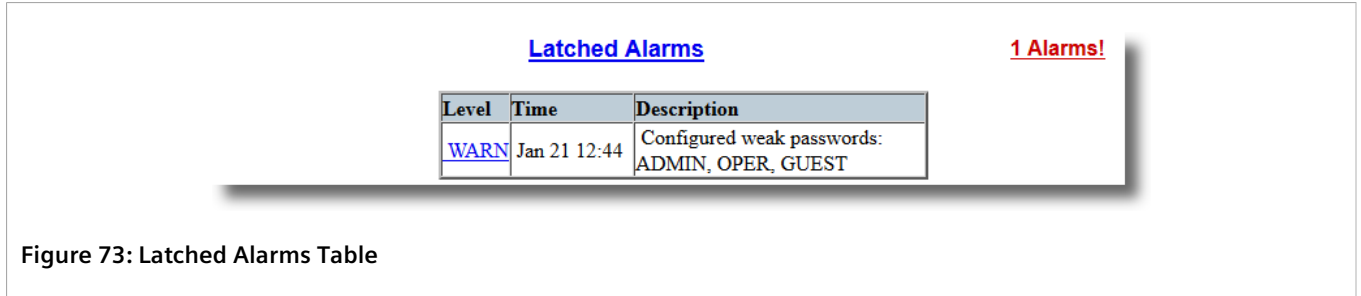
 **NOTE**  
 This list of alarms (configurable and non-configurable) is accessible through the Command Line Interface (CLI) using the **alarms**. For more information, refer to [Section 2.5.1, "Available CLI Commands"](#).

For information about modifying a pre-configured alarm, refer to [Section 5.4.3, "Configuring an Alarm"](#).

Section 5.4.2

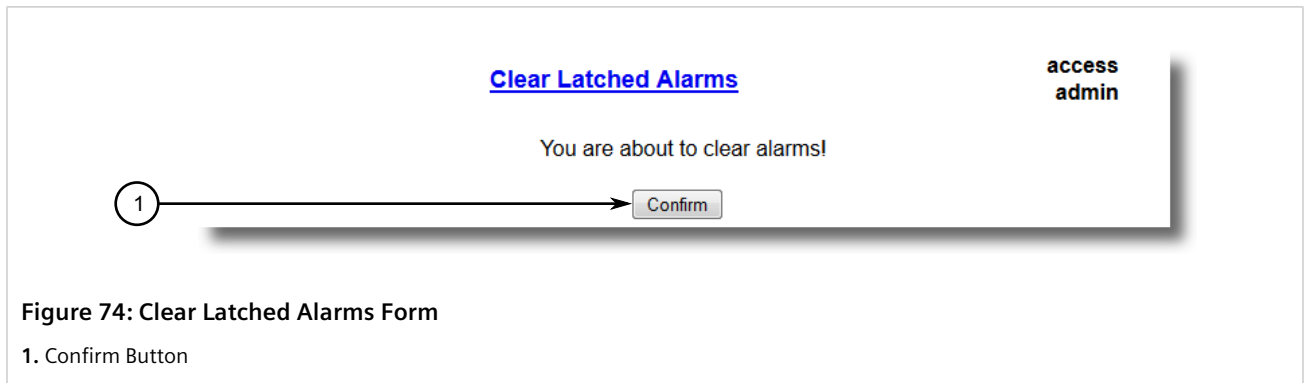
## Viewing and Clearing Latched Alarms

To view a list of alarms that are configured to latch, navigate to **Diagnostics » View Latched Alarms**. The **Latched Alarms** table appears.



To clear the passive alarms from the list, do the following:

1. Navigate to **Diagnostics » Clear Latched Alarms**. The **Clear Latched Alarms** form appears.



2. Click **Confirm**.

### Section 5.4.3

## Configuring an Alarm

While all alarms are pre-configured on the device, some alarms can be modified to suit the application. This includes enabling/disabling certain features and changing the refresh time.

To configuring an alarm, do the following:



**IMPORTANT!**

*Critical and Alert level alarms are not configurable and cannot be disabled.*

1. Navigate to **Diagnostic » Configure Alarms**. The **Alarms** table appears.

[access admin](#)

[Alarms](#)

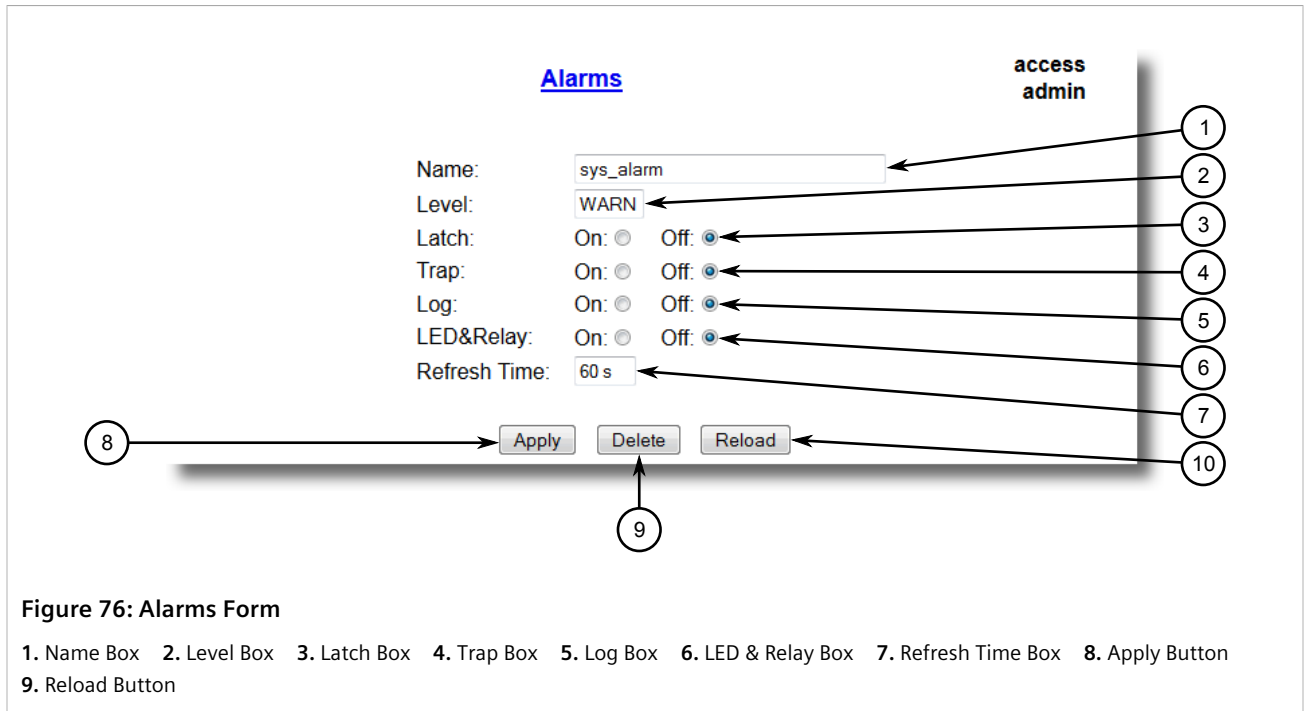
[InsertRecord](#)

Name	Level	Latch	Trap	Log	LED&Relay	Refresh Time
<a href="#">BPDU Guard activated</a>	ERRO	On	On	On	On	60 s
<a href="#">Can't create more mcast IP groups</a>	WARN	On	On	On	On	60 s
<a href="#">Clock manager alarm</a>	WARN	On	On	On	On	60 s
<a href="#">Configuration changed</a>	INFO	Off	On	On	Off	60 s
<a href="#">Default keys in use</a>	WARN	On	On	On	Off	0 s
<a href="#">Excessive failed login attempts</a>	WARN	On	On	On	On	60 s
<a href="#">GMRP cannot learn more addresses</a>	WARN	On	On	On	On	1 s
<a href="#">GVRP cannot learn more VLANs</a>	WARN	On	On	On	On	1 s
<a href="#">IEEE 1588 alarm</a>	WARN	On	On	On	On	60 s
<a href="#">Inconsistent speed/dpx in trunk</a>	ERRO	On	On	On	On	1 s

Figure 75: Alarms Table

2. Select an alarm. The **Alarms** form appears.





3. Configure the following parameter(s) as required:

Parameter	Description
Name	<b>Synopsis:</b> Any 34 characters <b>Default:</b> sys_alarm The alarm name, as obtained through the <code>alarms</code> CLI command.
Level	<b>Synopsis:</b> { EMRG, ALRT, CRIT, ERRO, WARN, NOTE, INFO, DEBG } Severity level of the alarm: <ul style="list-style-type: none"> <li>EMERG - The device has had a serious failure that caused a system reboot.</li> <li>ALERT - The device has had a serious failure that did not cause a system reboot.</li> <li>CRITICAL - The device has a serious unrecoverable problem.</li> <li>ERROR - The device has a recoverable problem that does not seriously affect operation.</li> <li>WARNING - Possibly serious problem affecting overall system operation.</li> <li>NOTIFY - Condition detected that is not expected or not allowed.</li> <li>INFO - Event which is a part of normal operation, e.g. cold start, user login etc.</li> <li>DEBUG - Intended for factory troubleshooting only.</li> </ul> This parameter is not configurable.
Latch	<b>Synopsis:</b> { On, Off } <b>Default:</b> Off Enables latching occurrence of this alarm in the Alarms Table.
Trap	<b>Synopsis:</b> { On, Off } <b>Default:</b> Off Enables sending an SNMP trap for this alarm.
Log	<b>Synopsis:</b> { On, Off } <b>Default:</b> Off Enables logging the occurrence of this alarm in syslog.txt.
LED & Relay	<b>Synopsis:</b> { On, Off } <b>Default:</b> Off

Parameter	Description
	Enables LED and fail-safe relay control for this alarm. If latching is not enabled, this field will remain disabled.
Refresh Time	<b>Synopsis:</b> 0 s to 60 s <b>Default:</b> 60 s Refreshing time for this alarm.

4. Click **Apply**.

#### Section 5.4.4

## Authentication Related Security Alarms

This section describes the authentication-related security messages that can be generated by RUGGEDCOM ROS.

### CONTENTS

- [Section 5.4.4.1, "Security Alarms for Login Authentication"](#)
- [Section 5.4.4.2, "Security Messages for Port Authentication"](#)

#### Section 5.4.4.1

### Security Alarms for Login Authentication

RUGGEDCOM ROS provides various logging options related to login authentication. A user can log into a RUGGEDCOM ROS device via four different methods: Web, console, SSH or Telnet. RUGGEDCOM ROS can log messages in the syslog, send a trap to notify an SNMP manager, and/or raise an alarm when a successful and unsuccessful login event occurs. In addition, when a weak password is configured on a unit or when the primary authentication server for TACACS+ or RADIUS is not reachable, RUGGEDCOM ROS will raise alarms, send SNMP traps and log messages in the syslog.

The following is a list of log and alarm messages related to user authentication:

- Weak Password Configured
- Login and Logout Information
- Excessive Failed Login Attempts
- RADIUS Server Unreachable
- TACACS Server Unreachable
- TACACS Response Invalid
- SNMP Authentication Failure



#### NOTE

*All alarms and log messages related to login authentication are configurable. For more information about configuring alarms, refer to [Section 5.4.3, "Configuring an Alarm"](#).*

#### » Weak Password Configured

RUGGEDCOM ROS generates this alarm and logs a message in the syslog when a weak password is configured in the **Passwords** table.

Message Name	Alarm	SNMP Trap	Syslog
Weak Password Configured	Yes	Yes	Yes

### » Default Keys In Use

RUGGEDCOM ROS generates this alarm and logs a message in the syslog when default keys are in use. For more information about default keys, refer to [Section 6.5, “Managing SSH and SSL Keys and Certificates”](#).

Message Name	Alarm	SNMP Trap	Syslog
Default Keys In Use	Yes	Yes	Yes

### » Login and Logout Information

RUGGEDCOM ROS generates this alarm and logs a message in the syslog when a successful and unsuccessful login attempt occurs. A message is also logged in the syslog when a user with a certain privilege level is logged out from the device.

Login attempts are logged regardless of how the user accesses the device (i.e. SSH, Web, Console, Telnet or RSH). However, when a user logs out, a message is only logged when the user is accessing the device through SSH, Telnet or Console.

Message Name	Alarm	SNMP Trap	Syslog
Successful Login	Yes	Yes	Yes
Failed Login	Yes	Yes	Yes
User Logout	No	No	Yes

### » Excessive Failed Login Attempts

RUGGEDCOM ROS generates this alarm and logs a message in the syslog after 10 failed login attempts by a user occur within a span of five minutes. Furthermore, the service the user attempted to access will be blocked for one hour to prevent further attempts.

Message Name	Alarm	SNMP Trap	Syslog
Excessive Failed Login Attempts	Yes	Yes	Yes

### » RADIUS Server Unreachable

RUGGEDCOM ROS generates this alarm and logs a message in the syslog when the primary RADIUS server is unreachable.

Message Name	Alarm	SNMP Trap	Syslog
Primary RADIUS Server Unreachable	Yes	Yes	Yes

### » TACACS+ Server Unreachable

RUGGEDCOM ROS generates this alarm and logs a message in the syslog when the primary TACACS+ server is unreachable.

Message Name	Alarm	SNMP Trap	Syslog
Primary TACACS Server Unreachable	Yes	Yes	Yes

### » TACACS+ Response Invalid

RUGGEDCOM ROS generate this alarm and logs a message in the syslog when the response from the TACACS+ server is received with an invalid CRC.

Message Name	Alarm	SNMP Trap	Syslog
TACACS Response Invalid	Yes	Yes	Yes

### » SNMP Authentication Failure

RUGGEDCOM ROS generates this alarm, sends an authentication failure trap, and logs a message in the syslog when an SNMP manager with incorrect credentials communicates with the SNMP agent in RUGGEDCOM ROS.

Message Name	Alarm	SNMP Trap	Syslog
SNMP Authentication Failure	Yes	Yes	Yes

#### Section 5.4.4.2

## Security Messages for Port Authentication

The following is the list of log and alarm messages related to port access control in RUGGEDCOM ROS:

- MAC Address Authorization Failure
- Secure Port X Learned MAC Addr on VLAN X
- Port Security Violated

### » MAC Address Authorization Failure

RUGGEDCOM ROS generates this alarm and logs a message in the syslog when a host connected to a secure port on the device is communicating using a source MAC address which has not been authorized by RUGGEDCOM ROS, or the dynamically learned MAC address has exceeded the total number of MAC addresses configured to be learned dynamically on the secured port. This message is only applicable when the port security mode is set to *Static MAC*.

Message Name	Alarm	SNMP Trap	Syslog
MAC Address Authorization Failure	Yes	Yes	Yes

### » Secure Port X Learned MAC Addr on VLAN X

RUGGEDCOM ROS logs a message in the syslog and sends a configuration change trap when a MAC address is learned on a secure port. Port X indicates the secured port number and VLAN number on that port. This message is not configurable in RUGGEDCOM ROS.

Message Name	SNMP Trap	Syslog
Secure Port X Learned MAC Addr on VLAN X	Yes	Yes

## » Port Security Violated

This message is only applicable when the security mode for a port is set to "802.1X or 802.1X/MAC-Auth"

RUGGEDCOM ROS this alarm and logs a message in the syslog when the host connected to a secure port tries to communicate using incorrect login credentials.

Message Name	Alarm	SNMP Trap	Syslog
802.1X Port X Authentication Failure	Yes	Yes	Yes
802.1X Port X Authorized Addr. XXX	No	No	Yes

### Section 5.5

## Managing the Configuration File

The device configuration file for RUGGEDCOM ROS is a single CSV (Comma-Separate Value) formatted ASCII text file, named `config.csv`. It can be downloaded from the device to view, compare against other configuration files, or store for backup purposes. It can also be overwritten by a complete or partial configuration file uploaded to the device.



#### NOTE

*The `config.csv` file is only available to admin users.*

#### CONTENTS

- [Section 5.5.1, "Updating the Configuration File"](#)

### Section 5.5.1

## Updating the Configuration File

Once downloaded from the device, the configuration file can be updated using a variety of different tools:



#### NOTE

*For information about uploading/downloading files, refer to [Section 4.4, "Uploading/Downloading Files"](#).*

- Any text editing program capable of reading and writing ASCII files
- Difference/patching tools (e.g. the UNIX `diff` and `patch` command line utilities)
- Source Code Control systems (e.g. CVS, SVN)

RUGGEDCOM ROS also has the ability to accept partial configuration updates. For example, to update only the parameters for Ethernet port 1 and leave all other parameters unchanged, transfer a file containing only the following lines to the device:

```
# Port Parameters
ethPortCfg
Port, Name, Media, State, AutoN, Speed, Dupx, FlowCtrl, LFI, Alarm,
1, Port 1, 100TX, Enabled, On, Auto, Auto, Off, Off, On,
```

# 6 Security

This chapter describes how to configure and manage the security-related features of RUGGEDCOM ROS.

## CONTENTS

- [Section 6.1, “Managing Passwords”](#)
- [Section 6.2, “Clearing Private Data”](#)
- [Section 6.3, “Managing User Authentication”](#)
- [Section 6.4, “Managing Port Security”](#)
- [Section 6.5, “Managing SSH and SSL Keys and Certificates”](#)

### Section 6.1

## Managing Passwords

RUGGEDCOM ROS allows for up to three user profiles to be configured locally on the device. Each profile corresponds to one of the following access levels:

- Guest
- Operator
- Admin

The access levels provide or restrict the user's ability to change settings and execute various commands.

Rights	User Type		
	Guest	Operator	Admin
View Settings	✓	✓	✓
Clear Logs	✗	✗	✓
Reset Alarms	✗	✓	✓
Clear Statistics	✗	✓	✓
Change Basic Settings	✗	✓	✓
Change Advanced Settings	✗	✗	✓
Run Commands	✗	✗	✓

Default passwords are configured for each user type initially. It is strongly recommended that these be changed before the device is commissioned.

**NOTE**  
Users can also be verified through a RADIUS or TACACS+ server. When enabled for authentication and authorization, the RADIUS or TACACS+ server will be used in the absence of any local settings. For more information about configuring a RADIUS or TACACS+ server, refer to [Section 6.3, "Managing User Authentication"](#).

**CAUTION!**  
To prevent unauthorized access to the device, make sure to change the default passwords for each profile before commissioning the device.

**CONTENTS**

- [Section 6.1.1, "Configuring Passwords"](#)
- [Section 6.1.2, "Resetting Passwords"](#)

Section 6.1.1

## Configuring Passwords

To configure passwords for one or more of the user profiles, do the following:

1. Navigate to **Administration » Configure Passwords**. The **Configure Passwords** form appears.


The screenshot shows the 'Configure Passwords' web form. At the top left is the title 'Passwords' in blue. On the right side, there is a vertical list of user profiles: 'access' and 'admin'. The form contains the following fields and controls:

- Auth Type: A dropdown menu currently set to 'Local' (callout 1).
- Guest Username: A text box containing 'guest' (callout 2).
- Guest Password: An empty text box (callout 3).
- Confirm Guest Password: An empty text box (callout 4).
- Operator Username: A text box containing 'operator' (callout 5).
- Operator Password: An empty text box (callout 6).
- Confirm Operator Password: An empty text box (callout 7).
- Admin Username: A text box containing 'admin' (callout 8).
- Admin Password: An empty text box (callout 9).
- Confirm Admin Password: An empty text box (callout 10).
- Password Reset Option: Radio buttons for 'Disabled' and 'Enabled', with 'Enabled' selected (callout 11).
- Password Minimum Length: A text box containing '1' (callout 12).
- At the bottom, there are two buttons: 'Apply' (callout 13) and 'Reload' (callout 14).

**Figure 77: Configure Passwords Form**

1. Auth Type Box 2. Guest Username Box 3. Guest Password Box 4. Confirm Guest Password Box 5. Operator Username Box  
6. Operator Password Box 7. Confirm Operator Password Box 8. Admin Username Box 9. Admin Password Box 10. Confirm Admin Password Box  
11. Password Reset Option 12. Password Minimum Length box 13. Apply Button 14. Reload Button






 **NOTE**  
RUGGEDCOM ROS requires that all user passwords meet strict guidelines to prevent the use of weak passwords. When creating a new password, make sure it adheres to the following rules:

- Must not be less than 8 characters in length.
- Must not include the username or any 4 continuous characters found in the username. For example, if the username is **Subnet25**, the password may not be **subnet25admin**, **subnetadmin** or **net25admin**. However, **net-25admin** or **Sub25admin** is permitted.
- Must have at least one alphabetic character and one number. Special characters are permitted.
- Must not have more than 3 continuously incrementing or decrementing numbers. For example, **Sub123** and **Sub19826** are permitted, but **Sub12345** is not.

An alarm will generate if a weak password is configured. The weak password alarm can be disabled by the user. For more information about disabling alarms, refer to [Section 5.4, "Managing Alarms"](#).

2. Configure the following parameter(s) as required:

Parameter	Description
Auth Type	<p><b>Synopsis:</b> { Local, RADIUS, TACACS+, RADIUSorLocal, TACACS+orLocal }</p> <p><b>Default:</b> Local</p> <p>Password can be authenticated using locally configured values, or remote RADIUS or TACACS+ server. Setting value to any of combinations that involve RADIUS or TACACS+ require Security Server Table to be configured.</p> <p>Settings:</p> <ul style="list-style-type: none"> <li>• Local - Authentication from the local Password Table.</li> <li>• RADIUS - Authentication using a RADIUS server.</li> <li>• TACACS+ - Authentication using a TACACS+ server.</li> <li>• RADIUSOrLocal - Authentication using RADIUS. If the server cannot be reached, authenticate from the local Password Table.</li> <li>• TACACS+OrLocal - Authentication using TACACS+. If the server cannot be reached, authenticate from the local Password Table</li> </ul>
	<p> <b>NOTE</b> For console access, local credentials will always be checked first regardless of the device configuration. If server authentication is required, requests to the server will be sent only if local authentication fails.</p>
Guest Username	<p><b>Synopsis:</b> Any 15 characters</p> <p><b>Default:</b> guest</p> <p>Related password is in field Guest Password; view only, cannot change settings or run any commands.</p>
Guest Password	<p><b>Synopsis:</b> 19 character ASCII string</p> <p>Related username is in field Guest Username; view only, cannot change settings or run any commands.</p>
Confirm Guest Password	<p><b>Synopsis:</b> 19 character ASCII string</p> <p>Related username is in field Guest Username; view only, cannot change settings or run any commands.</p>
Operator Username	<p><b>Synopsis:</b> Any 15 characters</p> <p><b>Default:</b> operator</p> <p>Related password is in field Oper Password; cannot change settings; can reset alarms, statistics, logs, etc.</p>

Parameter	Description
Operator Password	<p><b>Synopsis:</b> 19 character ASCII string</p> <p>Related username is in field Oper Username; cannot change settings; can reset alarms, statistics, logs, etc</p>
Confirm Operator Password	<p><b>Synopsis:</b> 19 character ASCII string</p> <p>Related username is in field Oper Username; cannot change settings; can reset alarms, statistics, logs, etc.</p>
Admin Username	<p><b>Synopsis:</b> Any 15 characters</p> <p><b>Default:</b> admin</p> <p>Related password is in field Admin Password; full read/write access to all settings and commands.</p>
Admin Password	<p><b>Synopsis:</b> 19 character ASCII string</p> <p>Related username is in field Admin Username; full read/write access to all settings and commands.</p>
Confirm Admin Password	<p><b>Synopsis:</b> 19 character ASCII string</p> <p>Related username is in field Admin Username; full read/write access to all settings and commands.</p>
Clear Private Data Option	<p><b>Synopsis:</b> { Disabled, Enabled }</p> <p><b>Default:</b> Enabled</p> <p>Enables or disables the feature of Clear Private Data. When enabled, during system boot up, a user with serial console access can clear all configuration data and keys stored on the device. In doing so, all user names and passwords are restored to factory defaults.</p> <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;"> <p> <b>NOTE</b> This provides the ability to reset password if lost or forgotten. If disabled, the device must be sent to Siemens Customer Support.</p> </div>
Password Minimum Length	<p><b>Synopsis:</b> 1 to 17</p> <p><b>Default:</b> 1</p> <p>Configure the password string minimum length. New passwords shorter than the minimum length will be rejected.</p> <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;"> <p> <b>IMPORTANT!</b> When this parameter is increased, all of the passwords must be set, even for a user level with a blank user name. The single minimum setting applies to all three passwords.</p> </div>

- Click **Apply**.

### Section 6.1.2

## Resetting Passwords

Passwords should be recorded in a secure location for future reference. For more information about authentication best practices, refer to [Section 1.2, "Security Recommendations"](#).

When the user name and/or password for the admin account is forgotten, a user with physical access to the device can restore all user names and passwords to factory default settings.

For more information about resetting passwords, refer to [Section 6.2, "Clearing Private Data"](#).

## Section 6.2

## Clearing Private Data

During system boot up, a user with serial console access can clear all configuration data and keys stored on the device, and restore all user names and passwords to factory default settings.

To clear private data, do the following:

**NOTE**

*The commands used in the following procedure are time-sensitive. If the specified time limits are exceeded before providing the appropriate response, the device will continue normal boot up.*

1. Make sure the *Clear Private Data Option* parameter is set to Enabled. For more information, refer to [Section 6.1.1, "Configuring Passwords"](#).
2. Connect to the device via the RS-232 serial console port. For more information, refer to [Section 3.1.2, "Connecting Directly"](#).
3. Cycle power to the device. As the device is booting up, the following prompt will appear:

```
Press any key to start
```

4. Within four seconds, press **CTRL + r**. The access banner will appear, followed by the command prompt:

```
>
```

5. Type the following command, then press **Enter** within 30 seconds:

```
clear private data
```

6. When prompted "Do you want to clear private data (Yes/No)?", answer yes and press **Enter** within five seconds. All configuration and keys in flash will be zeroized. An entry in the event log will be created. Crashlog.txt files (if existing) and syslog.txt files will be preserved. The device will reboot automatically.

## Section 6.3

## Managing User Authentication

This section describes the various methods for authenticating users.

**CONTENTS**

- [Section 6.3.1, "Managing RADIUS Authentication"](#)
- [Section 6.3.2, "Managing TACACS+ Authentication"](#)

## Section 6.3.1

### Managing RADIUS Authentication

RUGGEDCOM ROS can be configured to act as a RADIUS client and forward user credentials to a RADIUS (Remote Authentication Dial In User Service) server for remote authentication and authorization.

RADIUS is a UDP-based protocol used for carrying authentication, authorization and configuration information between a Network Access Server (NAS) that desires to authenticate its links and a shared authentication server. It provides centralized authentication and authorization for network access.

RADIUS is also widely used in conjunction with the IEEE 802.1X standard for port security using the Extensible Authentication Protocol (EAP).

**IMPORTANT!**

The RADIUS protocol is disabled by default in RUGGEDCOM ROS. To meet varied customer needs, this protocol can be enabled, but enabling it will break compliance with FIPS 140-2. For more information, refer to the **FIPS 140-2 Non-Proprietary Security Policy** or contact Siemens Customer Support.

**IMPORTANT!**

RADIUS messages are sent as UDP messages. The switch and the RADIUS server must use the same authentication and encryption key.

**IMPORTANT!**

RUGGEDCOM ROS supports both Protected Extensible Authentication Protocol (PEAP) and EAP-MD5. PEAP is more secure and is recommended if available in the supplicant.

**NOTE**

For more information about the RADIUS protocol, refer to [RFC 2865](http://tools.ietf.org/html/rfc2865) [<http://tools.ietf.org/html/rfc2865>].  
For more information about the Extensible Authentication Protocol (EAP), refer to [RFC 3748](http://tools.ietf.org/html/rfc3748) [<http://tools.ietf.org/html/rfc3748>].

**CONTENTS**

- [Section 6.3.1.1, "Configuring RADIUS Authentication"](#)
- [Section 6.3.1.2, "Configuring the RADIUS Server"](#)
- [Section 6.3.1.3, "Configuring the RADIUS Client on the Device"](#)

## Section 6.3.1.1

**Configuring RADIUS Authentication**

In a RADIUS access request, the following attributes and values are typically sent by the RADIUS client (RUGGEDCOM ROS) to the RADIUS server:

Attribute	Value
User-Name	{ Guest, Operator, Admin }
User-Password	{ password }
Service-Type	1
Vendor-Specific	Vendor-ID: 15004 Type: 1 Length: 11 String: RuggedCom

A RADIUS server may also be used to authenticate access on ports with 802.1x security support. When this is required, the following attributes are sent by the RADIUS client to the RADIUS server:

Attribute	Value
User-Name	{ The username as derived from the client's EAP identity response }

Attribute	Value
NAS-IP-Address	{ The Network Access Server IP address }
Service-Type	2
Frame-MTU	1500
EAP-Message <sup>a</sup>	{ A message(s) received from the authenticating peer }

<sup>a</sup> EAP-Message is an extension attribute for RADIUS, as defined by RFC 2869 [http://freeradius.org/rfc/rfc2869.html#EAP-Message].

To configure RADIUS authentication, do the following:

1. Configure the RADIUS Server. For more information, refer to [Section 6.3.1.2, “Configuring the RADIUS Server”](#).
2. Configure the RADIUS Client. For more information, refer to [Section 6.3.1.3, “Configuring the RADIUS Client on the Device”](#).

### Section 6.3.1.2

## Configuring the RADIUS Server



#### NOTE

For information about configuring the RADIUS server, refer to the manufacturer's instructions of the server being configured.

The Vendor-Specific attribute (or VSA) sent to the RADIUS server as part of the RADIUS request is used to determine the access level from the RADIUS server. This attribute may be configured within the RADIUS server with the following information:

Attribute	Value
Vendor-Specific	Vendor-ID: 15004 Format: String Number: 2 Attribute: { Guest, Operator, Admin }



#### NOTE

If no access level is received in the response packet from the RADIUS server, access is denied.

### Section 6.3.1.3

## Configuring the RADIUS Client on the Device

The RADIUS client can be configured to use two RADIUS servers: a primary server and a backup server. If the primary server is unavailable, the device will automatically attempt to connect with the backup server.



#### NOTE

The RADIUS client uses the Password Authentication Protocol (PAP) to verify access.

To configure access to either the primary or backup RADIUS servers, do the following:

1. Navigate to **Administration » Configure Security Server » Configure RADIUS Server**. The **RADIUS Server** table appears.

**RADIUS Server**

**access  
admin**

Server	IP Address	Auth UDP Port	Auth Key	Confirm Auth Key
<a href="#">Primary</a>		1812		
<a href="#">Backup</a>		1812		

**Figure 78: RADIUS Server Table**

- Select either **Primary** or **Backup** from the table. The **RADIUS Server** form appears.

**RADIUS Server**

Server:  ← 1

IP Address:  ← 2

Auth UDP Port:  ← 3

Auth Key:  ← 4

Confirm Auth Key:  ← 5

← 6     ← 7

**Figure 79: RADIUS Server Form**

1. Server Box   2. IP Address Box   3. Auth UDP Port Box   4. Auth Key Box   5. Confirm Auth Key Box   6. Apply Button   7. Reload Button

- Configure the following parameter(s) as required:

Parameter	Description
Server	<b>Synopsis:</b> Any 8 characters <b>Default:</b> Primary This field tells whether this configuration is for a Primary or a Backup Server.
IP Address	<b>Synopsis:</b> ###.###.###.### where ### ranges from 0 to 255 The Server IP Address.
Auth UDP Port	<b>Synopsis:</b> 1 to 65535 <b>Default:</b> 1812 The IP Port on server.
Auth Key	<b>Synopsis:</b> 31 character ASCII string The authentication key to be shared with server.
Confirm Auth Key	<b>Synopsis:</b> 31 character ASCII string The authentication key to be shared with server.

- Click **Apply**.

Section 6.3.2

## Managing TACACS+ Authentication

TACACS+ (Terminal Access Controller Access-Control System Plus) is a TCP-based access control protocol that provides authentication, authorization and accounting services to routers, Network Access Servers (NAS) and other networked computing devices via one or more centralized servers.



**IMPORTANT!**

The TACACS+ protocol is disabled by default in RUGGEDCOM ROS. To meet varied customer needs, this protocol can be enabled, but enabling it will break compliance with FIPS 140-2. For more information, refer to the **FIPS 140-2 Non-Proprietary Security Policy** or contact Siemens Customer Support.

**CONTENTS**

- [Section 6.3.2.1, "Configuring TACACS+"](#)
- [Section 6.3.2.2, "Configuring User Privileges"](#)

Section 6.3.2.1

### Configuring TACACS+

RUGGEDCOM ROS can be configured to use two TACACS+ servers: a primary server and a backup server. If the primary server is unavailable, the device will automatically attempt to connect with the backup server.

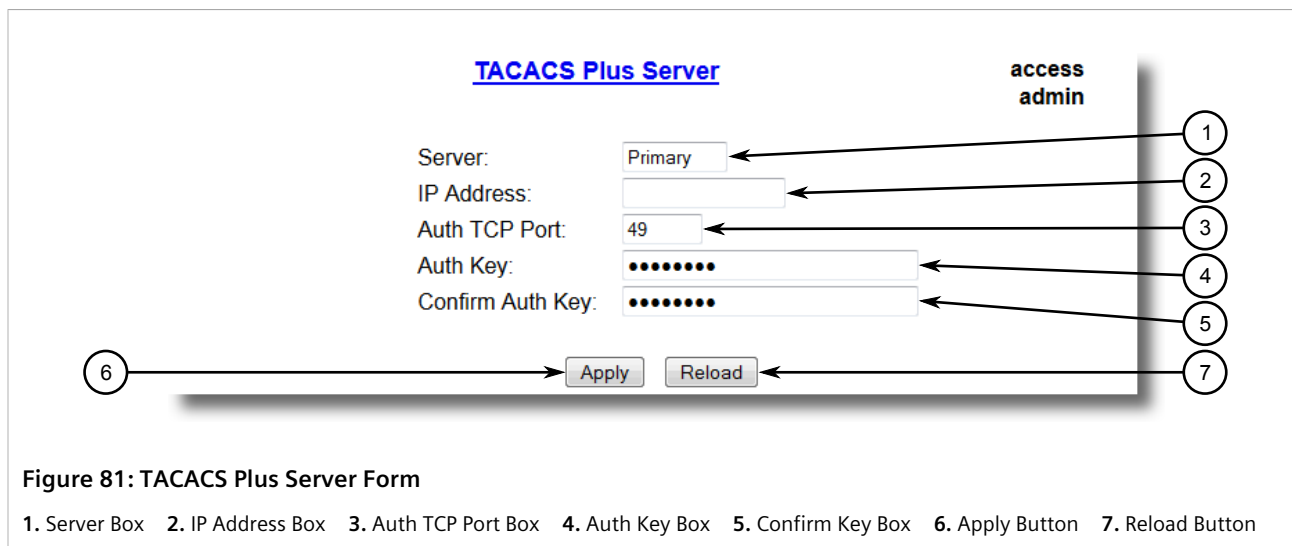
To configure access to either the primary or backup TACACS+ servers, do the following:

1. Navigate to **Administration » Configure Security Server » Configure TacPlus Server » Configure TACACS Plus Server**. The TACACS Plus Server table appears.

<u>TACACS Plus Server</u>				access admin
Server	IP Address	Auth TCP Port	Auth Key	Confirm Auth Key
<a href="#">Primary</a>		49	xxxxxxxx	xxxxxxxx
<a href="#">Backup</a>		49	xxxxxxxx	xxxxxxxx

Figure 80: TACACS Plus Server Table

2. Select either **Primary** or **Backup** from the table. The **TACACS Plus Server** form appears.



**Figure 81: TACACS Plus Server Form**

1. Server Box 2. IP Address Box 3. Auth TCP Port Box 4. Auth Key Box 5. Confirm Key Box 6. Apply Button 7. Reload Button

3. Configure the following parameter(s) as required:

Parameter	Description
Server	<b>Synopsis:</b> Any 8 characters <b>Default:</b> Primary This field tells whether this configuration is for a Primary or a Backup Server.
IP Address	<b>Synopsis:</b> ###.###.###.### where ### ranges from 0 to 255 The Server IP Address.
Auth TCP Port	<b>Synopsis:</b> 1 to 65535 <b>Default:</b> 49 The IP Port on server.
Auth Key	<b>Synopsis:</b> 31 character ascii string <b>Default:</b> mySecret The authentication key to be shared with server.
Confirm Auth Key	<b>Synopsis:</b> 31 character ascii string The authentication key to be shared with server.

4. Set the privilege levels for each user type (i.e. admin, operator and guest). For more information, refer to [Section 6.3.2.2, "Configuring User Privileges"](#).
5. Click **Apply**.

#### Section 6.3.2.2

### Configuring User Privileges

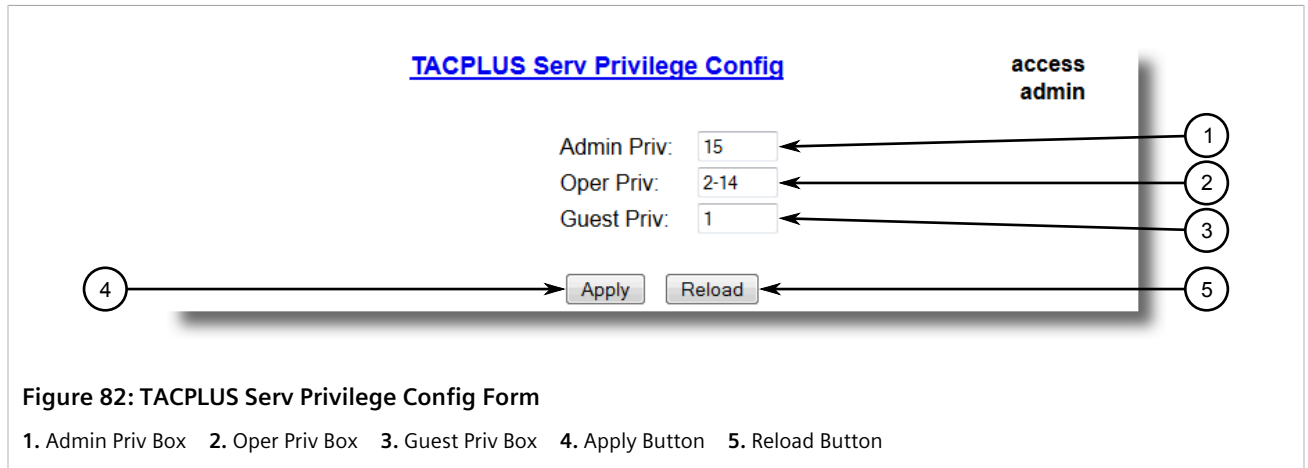
Each TACACS+ authentication request includes a *priv\_lvl* attribute that is used to grant access to the device. By default, the attribute uses the following ranges:

- 15 represents the *admin* access level
- 2-14 represents the *operator* access level
- 1 represents the *guest* access level



To configure the privilege levels for each user type, do the following:

1. Navigate to **Administration » Configure Security Server » Configure TacPlus Server » Configure TACPLUS Serv Privilege Config**. The TACPLUS Serv Privilege Config form appears.



2. Configure the following parameter(s) as required:

Parameter	Description
Admin Priv	<b>Synopsis:</b> (0 to 15)-(0 to 15) <b>Default:</b> 15 Privilege level to be assigned to the user.
Oper Priv	<b>Synopsis:</b> (0 to 15)-(0 to 15) <b>Default:</b> 2-14 Privilege level to be assigned to the user.
Guest Priv	<b>Synopsis:</b> (0 to 15)-(0 to 15) <b>Default:</b> 1 Privilege level to be assigned to the user.

3. Click **Apply**.

#### Section 6.4

## Managing Port Security

Port security, or port access control, provides the ability to filter or accept traffic from specific MAC addresses.

Port security works by inspecting the source MAC addresses of received frames and validating them against the list of MAC addresses authorized by the port. Unauthorized frames are filtered and, optionally, the port that received the frame can be shut down permanently or for a specified period of time. An alarm will be raised indicating the detected unauthorized MAC address.

Frames to unknown destination addresses are flooded through secure ports.

#### CONTENTS

- [Section 6.4.1, "Port Security Concepts"](#)
- [Section 6.4.2, "Viewing a List of Authorized MAC Addresses"](#)

- [Section 6.4.3, “Configuring Port Security”](#)
- [Section 6.4.4, “Configuring IEEE 802.1X”](#)

## Section 6.4.1

## Port Security Concepts

This section describes some of the concepts important to the implementation of port security in RUGGEDCOM ROS.

### CONTENTS

- [Section 6.4.1.1, “Static MAC Address-Based Authentication”](#)
- [Section 6.4.1.2, “IEEE 802.1x Authentication”](#)
- [Section 6.4.1.3, “IEEE 802.1X Authentication with MAC Address-Based Authentication”](#)
- [Section 6.4.1.4, “Assigning VLANs with Tunnel Attributes”](#)

## Section 6.4.1.1

### Static MAC Address-Based Authentication

With this method, the switch validates the source MAC addresses of received frames against the contents in the Static MAC Address Table.

RUGGEDCOM ROS also supports a highly flexible Port Security configuration which provides a convenient means for network administrators to use the feature in various network scenarios.

A Static MAC address can be configured without a port number being explicitly specified. In this case, the configured MAC address will be automatically authorized on the port where it is detected. This allows devices to be connected to any secure port on the switch without requiring any reconfiguration.

The switch can also be programmed to learn (and, thus, authorize) a pre-configured number of the first source MAC addresses encountered on a secure port. This enables the capture of the appropriate secure addresses when first configuring MAC address-based authorization on a port. Those MAC addresses are automatically inserted into the Static MAC Address Table and remain there until explicitly removed by the user.

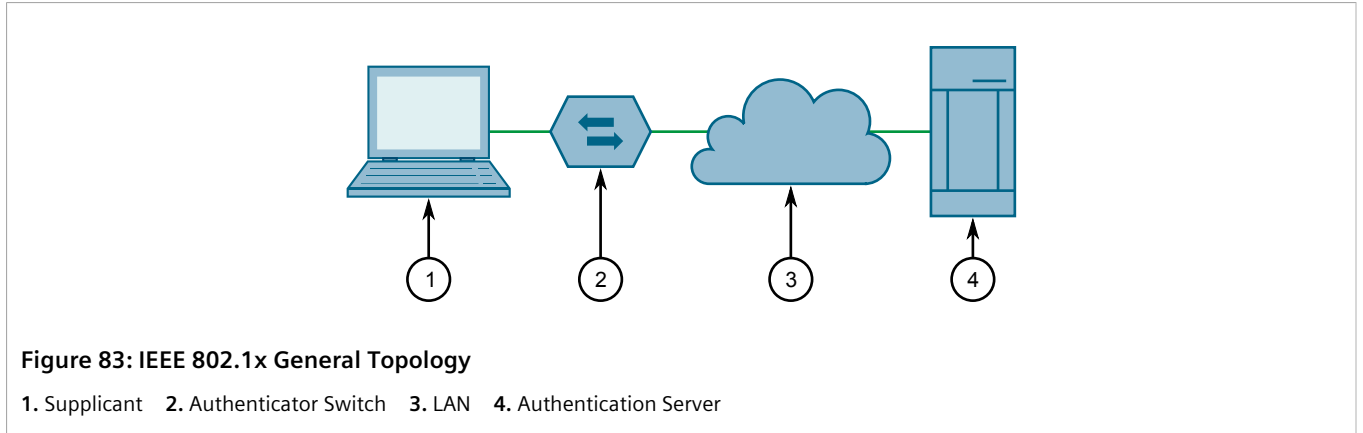
## Section 6.4.1.2

### IEEE 802.1x Authentication

The IEEE 802.1x standard defines a mechanism for port-based network access control and provides a means of authenticating and authorizing devices attached to LAN ports.

Although IEEE 802.1x is mostly used in wireless networks, this method is also implemented in wired switches.

The IEEE 802.1x standard defines three major components of the authentication method: Supplicant, Authenticator and Authentication server. RUGGEDCOM ROS supports the Authenticator component.



**Figure 83: IEEE 802.1x General Topology**

1. Supplicant 2. Authenticator Switch 3. LAN 4. Authentication Server



**IMPORTANT!**

*RUGGEDCOM ROS supports both Protected Extensible Authentication Protocol (PEAP) and EAP-MD5. PEAP is more secure and is recommended if available in the supplicant.*

IEEE 802.1x makes use of the Extensible Authentication Protocol (EAP), which is a generic PPP authentication protocol that supports various authentication methods. IEEE 802.1x defines a protocol for communication between the Supplicant and the Authenticator, referred to as EAP over LAN (EAPOL).

RUGGEDCOM ROS communicates with the Authentication Server using EAP over RADIUS.



**NOTE**

*The switch supports authentication of one host per port.*



**NOTE**

*If the host's MAC address is configured in the Static MAC Address Table, it will be authorized, even if the host authentication is rejected by the authentication server.*

Section 6.4.1.3

## IEEE 802.1X Authentication with MAC Address-Based Authentication

This method, also referred to as MAB (MAC-Authentication Bypass), is commonly used for devices, such as VoIP phones and Ethernet printers, that do not support the 802.1x protocol. This method allows such devices to be authenticated using the same database infrastructure as that used in 802.1x.

IEEE 802.1x with MAC-Authentication Bypass works as follows:

1. The device connects to a switch port.
2. The switch learns the device MAC address upon receiving the first frame from the device (the device usually sends out a DHCP request message when first connected).
3. The switch sends an EAP Request message to the device, attempting to start 802.1X authentication.
4. The switch times out while waiting for the EAP reply, because the device does not support 802.1x.
5. The switch sends an authentication message to the authentication server, using the device MAC address as the username and password.
6. The switch authenticates or rejects the device according to the reply from the authentication server.

## Section 6.4.1.4

## Assigning VLANS with Tunnel Attributes

RUGGEDCOM ROS supports assigning a VLAN to the authorized port using tunnel attributes, as defined in [RFC 3580](http://tools.ietf.org/html/rfc3580) [http://tools.ietf.org/html/rfc3580], when the Port Security mode is set to 802.1x or 802.1x/MAC-Auth.

In some cases, it may be desirable to allow a port to be placed into a particular VLAN, based on the authentication result. For example:

- To allow a particular device, based on its MAC address, to remain on the same VLAN as it moves within a network, configure the switches for 802.1X/MAC-Auth mode
- To allow a particular user, based on the user's login credentials, to remain on the same VLAN when the user logs in from different locations, configure the switches for 802.1X mode

If the RADIUS server wants to use this feature, it indicates the desired VLAN by including tunnel attributes in the Access-Accept message. The RADIUS server uses the following tunnel attributes for VLAN assignment:

- Tunnel-Type=VLAN (13)
- Tunnel-Medium-Type=802
- Tunnel-Private-Group-ID=VLANID

Note that VLANID is 12-bits and takes a value between 1 and 4094, inclusive. The Tunnel-Private-Group-ID is a string as defined in [RFC 2868](http://tools.ietf.org/html/rfc2868) [http://tools.ietf.org/html/rfc2868], so the VLANID integer value is encoded as a string.

If the tunnel attributes are not returned by the authentication server, the VLAN assigned to the switch port remains unchanged.

## Section 6.4.2

## Viewing a List of Authorized MAC Addresses

To view a list of static MAC addresses learned from secure ports, navigate to **Network Access Control » Port Security » View Authorized MAC Addresses**. The **Authorized MAC Addresses** table appears.

**NOTE**

Only MAC addresses authorized on a static MAC port(s) are shown. MAC addresses authorized with IEEE 802.1X are not shown.

**Authorized MAC Addresses**access  
admin

Port	MAC Address	VID	Sticky
1	00-00-00-00-00-03	1	No

Figure 84: Authorized MAC Addresses Table

This table displays the following information:

Parameter	Description
Port	<b>Synopsis:</b> 1 to maximum port number Port on which MAC address has been learned.
MAC Address	<b>Synopsis:</b> ##-##-##-##-##-## where ## ranges 0 to FF

Parameter	Description
	Authorized MAC address learned by the switch.
VID	<b>Synopsis:</b> 0 to 65535 VLAN Identifier of the VLAN upon which the MAC address operates.
Sticky	<b>Synopsis:</b> { No, Yes } This describes whether the authorized MAC address/Device can move to another port or not: <ul style="list-style-type: none"> <li>• YES - authorized MAC address/Device cannot move to a different switch port</li> <li>• NO - authorized MAC address/Device may move to another switch port</li> </ul>

If a MAC address is not listed, do the following:

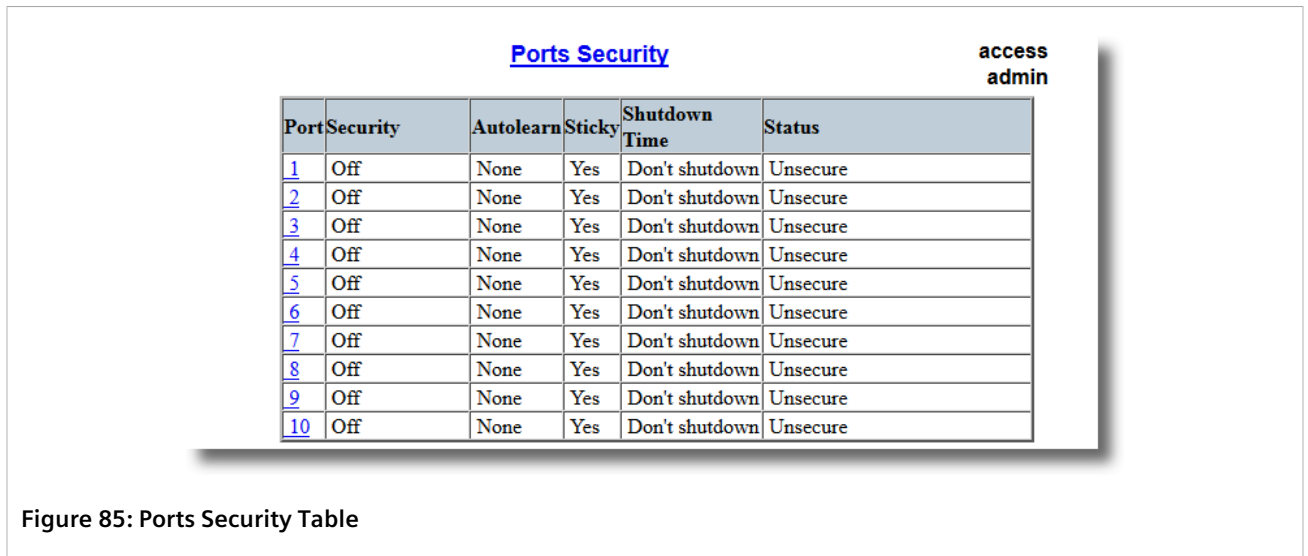
- Configure port security. For more information, refer to [Section 6.4.3, "Configuring Port Security"](#).
- Configure IEEE 802.1X. For more information, refer to [Section 6.4.4, "Configuring IEEE 802.1X"](#).

Section 6.4.3

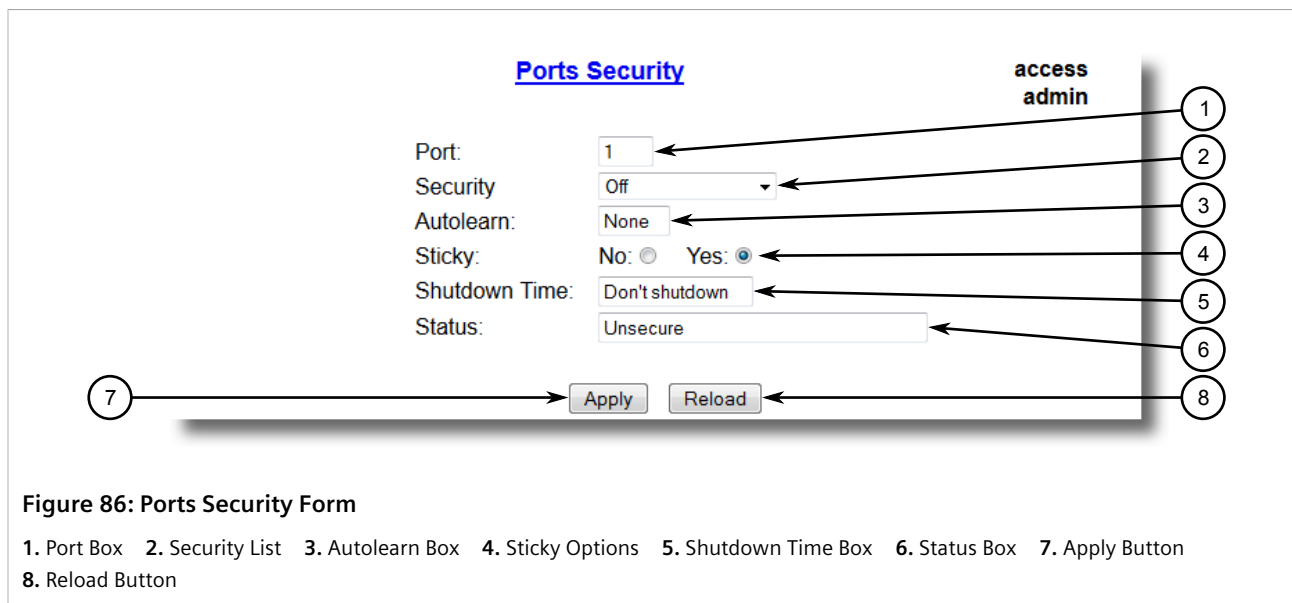
## Configuring Port Security

To configure port security, do the following:

1. Navigate to **Network Access Control » Port Security » Configure Ports Security**. The **Ports Security** table appears.



2. Select an Ethernet port. The **Ports Security** form appears.



**Figure 86: Ports Security Form**

1. Port Box   2. Security List   3. Autolearn Box   4. Sticky Options   5. Shutdown Time Box   6. Status Box   7. Apply Button  
8. Reload Button

3. Configure the following parameter(s) as required:

Parameter	Description
Port	<b>Synopsis:</b> 1 to maximum port number <b>Default:</b> 1 The port number as seen on the front plate silkscreen of the switch.
Security	<b>Synopsis:</b> { Off, Static MAC, 802.1X, 802.1X/MAC-Auth } <b>Default:</b> Off Enables or disables the port's security feature. Two types of port access control are available: <ul style="list-style-type: none"> <li>• Static MAC address-based. With this method, authorized MAC address(es) should be configured in the Static MAC Address table. If some MAC addresses are not known in advance (or it is not known to which port they will be connected), there is still an option to configure the switch to auto-learn certain number of MAC addresses. Once learned, they do not age out until the unit is reset or the link goes down.</li> <li>• IEEE 802.1X standard authentication.</li> <li>• IEEE 802.1X with MAC-Authentication, also known as MAC-Authentication Bypass. With this option, the device can authenticate clients based on the client's MAC address if IEEE 802.1X authentication times out.</li> </ul>
Autolearn	<b>Synopsis:</b> 1 to 16 or { None } <b>Default:</b> None Only applicable when the 'Security' field has been set to 'Static MAC'. It specifies maximum number of MAC addresses that can be dynamically learned on the port. If there are static addresses configured on the port, the actual number of addresses allowed to be learned is this number minus the number of the static MAC addresses.
Sticky	<b>Synopsis:</b> { No, Yes } <b>Default:</b> Yes Only applicable when the 'Security' field has been set to 'Static MAC'. Change the behaviour of the port to either sticky or non-sticky. If Sticky is 'Yes', MACs/Devices authorized on the port 'stick' to the port and the switch will not allow them to move to a different port. If Sticky is 'No', MACs/Devices authorized on the port may move to another port.
Shutdown Time	<b>Synopsis:</b> 1 to 86400 s or { Until reset, Don't shutdown } <b>Default:</b> Don't shutdown

Parameter	Description
	Specifies for how long to shut down the port, if a security violation occurs.
Status	<b>Synopsis:</b> Any 31 characters Describes the security status of the port.

**i** **NOTE**  
There are a few scenarios in which static MAC addresses can move:

- When the link is up/down on a **non-sticky** secured port
- When traffic switches from or to a **non-sticky** secured port

**i** **NOTE**  
Traffic is lost until the source MAC Address of the incoming traffic is authorized against the static MAC address table.

4. Click **Apply**.

Section 6.4.4

## Configuring IEEE 802.1X

To configure IEEE 802.1X port-based authentication, do the following:

1. Navigate to **Network Access Control » Port Security » Configure 802.1X**. The **802.1X Parameters** table appears.

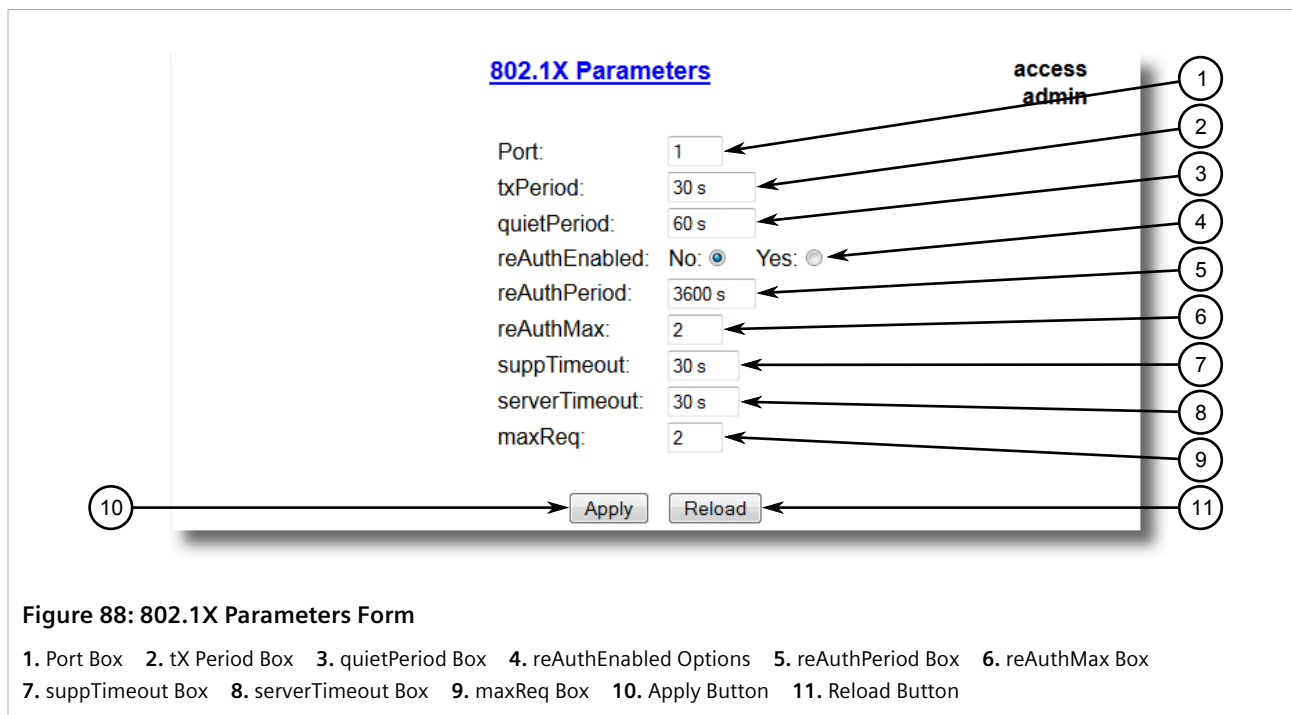
**802.1X Parameters**

access admin

Port	txPeriod	quietPeriod	reAuthEnabled	reAuthPeriod	reAuthMax	suppTimeout	serverTimeout	maxReq
<a href="#">1</a>	30 s	60 s	No	3600 s	2	30 s	30 s	2
<a href="#">2</a>	30 s	60 s	No	3600 s	2	30 s	30 s	2
<a href="#">3</a>	30 s	60 s	No	3600 s	2	30 s	30 s	2
<a href="#">4</a>	30 s	60 s	No	3600 s	2	30 s	30 s	2
<a href="#">5</a>	30 s	60 s	No	3600 s	2	30 s	30 s	2
<a href="#">6</a>	30 s	60 s	No	3600 s	2	30 s	30 s	2
<a href="#">7</a>	30 s	60 s	No	3600 s	2	30 s	30 s	2
<a href="#">8</a>	30 s	60 s	No	3600 s	2	30 s	30 s	2
<a href="#">9</a>	30 s	60 s	No	3600 s	2	30 s	30 s	2
<a href="#">10</a>	30 s	60 s	No	3600 s	2	30 s	30 s	2

**Figure 87: 802.1X Parameters Table**

2. Select an Ethernet port. The **802.1X Parameters** form appears.



**Figure 88: 802.1X Parameters Form**

1. Port Box 2. tX Period Box 3. quietPeriod Box 4. reAuthEnabled Options 5. reAuthPeriod Box 6. reAuthMax Box  
7. suppTimeout Box 8. serverTimeout Box 9. maxReq Box 10. Apply Button 11. Reload Button

3. Configure the following parameter(s) as required:

Parameter	Description
Port	<b>Synopsis:</b> 1 to maximum port number <b>Default:</b> 1 The port number as seen on the front plate silkscreen of the switch.
txPeriod	<b>Synopsis:</b> 1 to 65535 <b>Default:</b> 30 s The time to wait for the Supplicant's EAP Response/Identity packet before retransmitting an EAP Request/Identity packet.
quietPeriod	<b>Synopsis:</b> 0 to 65535 <b>Default:</b> 60 s The period of time not to attempt to acquire a Supplicant after the authorization session failed.
reAuthEnabled	<b>Synopsis:</b> { No, Yes } <b>Default:</b> No Enables or disables periodic re-authentication.
reAuthPeriod	<b>Synopsis:</b> 60 to 86400 <b>Default:</b> 3600 s The time between periodic re-authentication of the Supplicant.
reAuthMax	<b>Synopsis:</b> 1 to 10 <b>Default:</b> 2 The number of re-authentication attempts that are permitted before the port becomes unauthorized.
suppTimeout	<b>Synopsis:</b> 1 to 300 <b>Default:</b> 30 s The time to wait for the Supplicant's response to the authentication server's EAP packet.
serverTimeout	<b>Synopsis:</b> 1 to 300



Parameter	Description
	<b>Default:</b> 30 s The time to wait for the authentication server's response to the Supplicant's EAP packet.
maxReq	<b>Synopsis:</b> 1 to 10 <b>Default:</b> 2 The maximum number of times to retransmit the authentication server's EAP Request packet to the Supplicant before the authentication session times out.

4. Click **Apply**.

## Section 6.5

## Managing SSH and SSL Keys and Certificates

RUGGEDCOM ROS uses public key cryptography to establish secure remote logins (SSH) and Web access (SSL), in compliance with RFC 5280.

**IMPORTANT!**

*Secure web service files are not pre-configured at the factory; they must be prepared and provisioned by the administrator before the web server will start.*

RUGGEDCOM ROS secure web service requires the following items to be provisioned:

1. Trust store (`sslpub.certs`). Must contain at least one CA certificate in `sslpub.certs` (root or intermediate).
2. Server certificate (`ssl.crt`). A TLS server certificate and, optionally, a chain of intermediate issuing CA certificates, the last of which must have been issued by one of the CA certificates in the trust store. The server certificate must ultimately trace its authority and authenticity to the trust store.
3. The private PKI key that corresponds to the server certificate.

**NOTE**

*Only admin users can write certificates and keys to the device.*

**CONTENTS**

- [Section 6.5.1, "SSL Certificates"](#)
- [Section 6.5.2, "SSH Host Key"](#)
- [Section 6.5.3, "Managing SSH Public Keys"](#)
- [Section 6.5.4, "Generating a Certificate Signing Request \(CSR\)"](#)
- [Section 6.5.5, "Certificate and Key Examples"](#)

## Section 6.5.1

## SSL Certificates

**IMPORTANT!**

All CA certificates must set the CA flag to **TRUE**, and the server certificate must have the Server Authentication purpose (*id-kp 1* with OID 1.3.6.1.5.5.7.3.1) in the **extendedKeyUsage** field.

RUGGEDCOM ROS supports SSL certificates that conform to the following specifications:

- X.509 v3 digital certificate format
- PEM format
- RSA key pair, 2048 or 3072 bits

### » **ssl.crt**

The server certificate and all intermediates in `ssl.crt` must be configured with OCSP responder URIs to check revocation status. Specifically, each certificate must have an *authority info access* value containing an OCSP responder URI in the *subject alternative name* extension.

If RUGGEDCOM ROS receives an OCSP response indicating that one of the certificates in `ssl.crt` has been revoked, it will delete the `ssl.crt` file (irrespective of the setting of *OCSP Unreachable Action*).

If RUGGEDCOM ROS is unable to reach one of the OCSP responders, and the *OCSP Unreachable Action* parameter is set to *Reject*, then the `ssl.crt` file is deleted. Conversely, if the *OCSP Unreachable Action* parameter is set to *Accept*, no action is taken. For more information about the *OCSP Unreachable Action* parameter, refer to [Section 4.10, "Configuring IP Services"](#).

The `ssl.crt` file must contain at least the web server certificate, followed by its corresponding private key in PEM format.

The `ssl.crt` file may also contain a certification chain, i.e. a chain of issuing CA certificates. Each certificate in sequence must be the issuer of the certificate preceding it. The last of these must be verifiable as having been issued by one of the CA certificates in the trust store. A certificate chain in the `ssl.crt` file must conform to the following sequence:

1. The web server certificate
2. One or more issuing CA certificates, in issuing sequence
3. The web server certificate's private key

A unique SSL certificate must be created and uploaded to RUGGEDCOM ROS. The SSL certificate must be signed by either a trusted third-party Certificate Authority (CA) or by an organization's own CA.

### » **Trust Store (sslpub.certs)**

RUGGEDCOM ROS accepts one or more CA (Certificate Authority) certificates in the file `sslpub.certs`. The contents of this file make up the trust store. The following types of certificates may be included in `sslpub.certs`:

1. Intermediate certificates that act as a trust anchor to the server certificate in `ssl.crt`.
2. Root certificates that act as a trust anchor to all the intermediate certificates up to the server certificate in `ssl.crt`.
3. Online Certificate Status Protocol (OCSP) trusted responder certificates that can be used to verify OCSP responses.

Uploaded signed certificates and OSCP responses must ultimately trace their authority and authenticity to one of the CA certificates in the trust store. If the system has no valid `ssl.crt` certificate, SSL connection negotiation is disabled and therefore the web server is disabled.

**IMPORTANT!**

*Uploading `sslpub.certs` triggers a full re-validation of `ssl.crt`.*

## Section 6.5.2

## SSH Host Key

The RUGGEDCOM ROS SSH server can perform public key user authentication in addition to the traditional system password authentication.

**NOTE**

*SSH is not supported in Non-Controlled (NC) versions of RUGGEDCOM ROS.*

Controlled versions of RUGGEDCOM ROS support SSH public/private key pairs that conform to the following specifications:

- PEM format
- RSA key pair, 2048 or 3072 bits in length

## Section 6.5.3

## Managing SSH Public Keys

RUGGEDCOM ROS allows admin users to list, add and delete SSH public keys. Public keys are added as non-volatile storage (i.e. flash) files on RUGGEDCOM ROS devices, and are retrieved at the time of SSH client authentication.

**CONTENTS**

- [Section 6.5.3.1, "Public Key Requirements"](#)
- [Section 6.5.3.2, "Adding a Public Key"](#)
- [Section 6.5.3.3, "Viewing a List of Public Keys"](#)
- [Section 6.5.3.4, "Updating a Public Key"](#)
- [Section 6.5.3.5, "Deleting a Public Key"](#)

## Section 6.5.3.1

### Public Key Requirements

Public keys are stored in a flash file, called `sshpуб.keys`. The `sshpуб.keys` file consists of ssh user public key entries. Similar to the `config.csv` file, each entry must be separated by an empty line. An entry has two components. They are, in sequence:

- Header
- Key

The header contains the parameters of the entry, separated by comma. The parameters are, in sequence:

- ID: A number between 0 and 9999
- Entry type: UserKey
- Access Level: (Admin, Operator or Guest)
- Revocation Status: active/inactive (always active for keys)
- User Name: This is the client's user name (not the RUGGEDCOM ROS user name). This will be used by clients to later SSH into the RUGGEDCOM ROS device.

The key must be in RFC4716 format, or in PEM format with any of the following header and footer lines:

```
-----BEGIN PUBLIC KEY-----  
-----END PUBLIC KEY-----  
  
-----BEGIN SSH2 PUBLIC KEY-----  
-----END SSH2 PUBLIC KEY-----  
  
-----BEGIN RSA PUBLIC KEY-----  
-----END RSA PUBLIC KEY-----
```

The following is an example of a valid entry in the `sshpub.keys` file in PEM format:

```
1,userkey,admin,active,alice  
---- BEGIN SSH2 PUBLIC KEY ----  
AAAAB3NzaC1yc2EAAAABIwAAAQEA4mRrQfk+RKXnmGRvzMyWVDSbq5VwpGGrlLQYCrjVEa  
NdbXsphqYKop8V5VUeXFRAUFzOy82yk8TF/5JxGPWq6wRNjhnYR7IY2AiMBq0+K8XeUR1/  
z5K2XNRjnqTzSfWkhaUVJeduvjGgOlNN4yvgUwF3n0idU9k3E1q/na+LmYIeGhOwzCqoAc  
ipHAdR4fhD5u0jbmjv+gDikTSZlBj9eFJfP09ekImMLHwbBry0SSBpqAKbwVdWEXIKQ47  
zz7ao2/rs3rSV16IXSq3Qe8VZh2irah0Md6JFMOX2qm9fo1I62q1DDgheCOsOiGPf4xerH  
rI2cs6FT31rAdx2JOjvw==  
---- END SSH2 PUBLIC KEY ----
```

The following is an example of a valid entry in the `sshpub.keys` file in in RFC4716 format:

```
2,userkey,admin,active,bob  
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQGDH0NivR8zzbTxlcVFPzR/  
GR24NrRJa0Lc7scNsWRgi0XulHuGrRLRB5RoQ39+spdig88Y8CqhRI49XJx7uLJe0Su3RvyNYz1jkdSwHq2hSZCpukJxJ6CK95Po/  
sVa5Gq2qMaHowiYDSkcx+AJyWzK/eM6i/jc1251RxFPdfkj74u+ob3PCvmIWz5z3WAJBrQU1IDPHDets511WMu809/  
mAPZRwjqRWhRsQmcXZuv5oo54wIopCAZSo20SPz2VmXFuUsEwDkvYMXLJK1koJPbDjH7yFFC7mwK2eMU/  
oMFFn934cb05N6etsJSvplYQ4pMCw60k8Q/bB5cPSOa/rAt bob@work
```

RUGGEDCOM ROS allows only 16 user key entries to be stored. Each key entry must meet the following limits:

- Key size must not exceed 4000 base64 encoded characters
- Entry Type in the header must not exceed 8 ASCII characters
- Access Level in the header must not exceed 8 ASCII characters (*operator* is maximum)
- Revocation status in the header must not exceed 8 ASCII characters (*inactive* is maximum)
- User Name must not exceed 12 ASCII characters

### Section 6.5.3.2

## Adding a Public Key

Administrators can add one or more public keys to RUGGEDCOM ROS.

There are two ways to update `sshpub.keys`:

- Upload a locally-created file directly to the `sshpup.keys` file. The content of the file replace the content currently stored in flash memory.
- Upload a locally-created file to the `sshaddpub.keys` file. The content of the file is appended to the existing entries in the `sshpup.keys` file.

**IMPORTANT!**

The content of the `sshaddpub.keys` file must follow the same syntax as the `sshpup.keys` file.

To add keys, do the following:

1. Create a public key file via a host computer.
2. Transfer the public key file to the device using SFTP or Xmodem. For more information about transferring files, refer to [Section 4.4, “Uploading/Downloading Files”](#).
3. Log in to the device as an admin user and access the CLI shell. For more information about accessing the CLI shell, refer to [Section 2.5, “Using the Command Line Interface”](#).
4. Check the system log to make sure the files were properly transferred. For more information about viewing the system log, refer to [Section 4.5.1, “Viewing Local and System Logs”](#).

## Section 6.5.3.3

## Viewing a List of Public Keys

Admin users can view a list of existing public keys on the device.

To view public keys, do the following:

1. Log in to the device as an admin user and access the CLI shell. For more information about accessing the CLI shell, refer to [Section 2.5, “Using the Command Line Interface”](#).
2. At the CLI prompt, type:

```
sshpupkey list
```

A list of public keys will appear, including their key ID, access level, revocation status, user name and key fingerprint.

## Section 6.5.3.4

## Updating a Public Key

Admin users can update public keys.


To update public keys, do the following:

1. Log in to the device as an admin user and access the CLI shell. For more information about accessing the CLI shell, refer to [Section 2.5, “Using the Command Line Interface”](#).
2. At the CLI prompt, type:

```
sshpupkey list
```

A list of public keys will appear, including their key ID, access level, revocation status, user name and key fingerprint.

3. Type the following commands to update the public keys:

Command	Description
<code>sshpubkey update_id current_ID new_ID</code>	Updates the ID of user public key. <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;">  <b>NOTE</b>  <i>The user public key ID must be a number between 0 and 9999.</i> </div> <ul style="list-style-type: none"> <li>• <code>current_ID</code> is the ID currently assigned to the public key</li> <li>• <code>new_ID</code> is the ID that will be used to identify the public key going forward</li> </ul>
<code>sshpubkey update_al AL</code>	Updates the access level of a user public key. <ul style="list-style-type: none"> <li>• <code>AL</code> is the access level (admin, operator or guest) of the public key to be updated</li> </ul>
<code>sshpubkey update_rs RS</code>	Updates the revocation status (active, inactive) of a user public key. <ul style="list-style-type: none"> <li>• <code>RS</code> is the revocation status of the public key to be updated</li> </ul>
<code>sshpubkey update_un UN</code>	Updates the user name of a user public key. <ul style="list-style-type: none"> <li>• <code>UN</code> is the user name of the public key to be updated</li> </ul>

## Section 6.5.3.5

## Deleting a Public Key

Admin users can delete one or more public keys.

To delete a public key, do the following:

1. Log in to the device as an admin user and access the CLI shell. For more information about accessing the CLI shell, refer to [Section 2.5, "Using the Command Line Interface"](#).
2. At the CLI prompt, type:

```
sshpubkey list
```

A list of public keys will appear, including access level, revocation status, user name and key fingerprint.

3. Type the following commands to delete the public key(s):

Command	Description
<code>sshpubkey remove ID</code>	Removes a key from the non-volatile storage. <ul style="list-style-type: none"> <li>• <code>ID</code> is the ID of the public key to be removed</li> </ul>

## Section 6.5.4

## Generating a Certificate Signing Request (CSR)

RUGGEDCOM ROS can generate certificate signing requests.

The generated CSR will require a signature by a trusted third-party Certificate Authority (CA) or by an organization's own CA.


**NOTE**

*CSR generation can take up to two hours to complete. For faster generation, Siemens recommends using OpenSSL via PC to generate CSRs.*



**WARNING!**

The `csr.txt` file holds the private key in a readable format. For security, once the CSR has been uploaded to the CA where the certificate will be created, the `csr.txt` file will automatically be deleted from RUGGEDCOM ROS. It is the user's responsibility to store the contents of `csr.txt` securely for future use.

To generate a CSR, do the following:

1. Navigate to **Administration » Generate Certificate Signing Request**. The **Certificate Signing Request** form appears.

**Certificate Signing Request**

access admin

Key: RSA2048:  RSA3072:

Name:

Email:

Organization:

Department:

Locality:

State:

Country:

Figure 89: Certificate Signing Request Form

1. Key Options 2. Name Box 3. Email Box 4. Organization Box 5. Department Box 6. Locality Box 7. State Box 8. Country Box 9. Apply Button 10. Reload Button

2. Configure the following parameter(s) as required:

Parameter	Description
Key	<b>Synopsis:</b> { RSA2048, RSA3072 } Key type and size.
Name	<b>Synopsis:</b> Any 31 characters Common Name, for unique identification.
Email	<b>Synopsis:</b> Any 31 characters Email address for contact.
Organization	<b>Synopsis:</b> Any 15 characters Organization, business, or company name.
Department	<b>Synopsis:</b> Any 15 characters Organizational unit or department name.
Locality	<b>Synopsis:</b> Any 15 characters Locality, city, or town name.
State	<b>Synopsis:</b> Any 15 characters

Parameter	Description
	State, province, territory, or region name.
Country	<b>Synopsis:</b> Any 7 characters Country name, usually a two-letter ISO country code.

### 3. Click **Apply**.

The CSR and a corresponding private key will be generated and saved to the file `csr.txt`.

## Section 6.5.5

# Certificate and Key Examples

For SSL, certificates must meet the requirements outlined in [Section 6.5.1, “SSL Certificates”](#).

The certificate and keys must be combined in a single `ssl.crt` file and uploaded to the device.

The following is an abbreviated example of a combined SSL certificate and private key:

```
-----BEGIN CERTIFICATE-----
MIIFfzCCA+egAwIBAgICEAIwDQYJKoZIhvcNAQENBQAwfzELMAkGA1UEBhMCQ0Ex...
6GFzRWjt8RjRyJwkOkN7zkY0aA==
-----END CERTIFICATE-----
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAACAQEArjC57m7YRj1vqZ7f6/iPEd/2ZR8qXyMKAB5XzSFTK/svX8Lx...
iigfmoWFeWdaUXzWA3AlJsN12lmOSkEEYmbJGDUvbfL8qbE/wGpZaQ==
-----END RSA PRIVATE KEY-----
```

The following is an abbreviated example of an `sslpub.certs` file:

```
1000,active,rootca
-----BEGIN CERTIFICATE-----
MIIC8jCCAlSgAwIBAgIJAkhYdGaitTDoMAoGCCqGSM49BAMEMIGJMqswCQYDVQQG...
Ml9J1yV9BV4BWOBtoMsVUZ+Tf3liZ9nJUZNdhpx2ICFKR2DASsQ=
-----END CERTIFICATE-----
```

The following is an abbreviated example of an `sslpub.certs` file, including the certificate chain:

```
1000,active,rootca
-----BEGIN CERTIFICATE-----
MIIE8DCCA1igAwIBAgIJA04zUfv/K6n8MA0GCSqGSIb3DQEBCwUAMIGEMQswCQYD...
4uKTt6n2nBK5bp6ldXPPIeDHH20=
-----END CERTIFICATE-----
```

The following is an abbreviated example of an RSA key:

```
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAACAQEAA3Yy8uImwq+L2a9IqE0ckXVQqktfhxvAKVKdAqpl+QPJs003E...
YaQ5vVwbz6pOcTfXhdvmcZ3k6jEAAHKuKts3Zuz1f/X3PKzB/VU=
-----END RSA PRIVATE KEY-----
```



# 7 Layer 2

This chapter describes the Layer 2, or Data Link Layer (DLL), features of RUGGEDCOM ROS.

## CONTENTS

- [Section 7.1, “Managing Virtual LANs”](#)
- [Section 7.2, “Managing MAC Addresses”](#)
- [Section 7.3, “Managing Multicast Filtering”](#)

### Section 7.1

## Managing Virtual LANs

A Virtual Local Area Network (VLAN) is a group of devices on one or more LAN segments that communicate as if they were attached to the same physical LAN segment. VLANs are extremely flexible because they are based on logical connections, rather than physical connections.

When VLANs are introduced, all traffic in the network must belong to one VLAN or another. Traffic on one VLAN cannot pass to another, except through an inter-network router or Layer 3 switch.

VLANs are created in three ways:

- **Explicitly**  
Static VLANs can be created in the switch. For more information about static VLANs, refer to [Section 7.1.5, “Managing Static VLANs”](#).
- **Implicitly**  
When a VLAN ID (VID) is set for a port-based VLAN, static MAC address or IP interface, an appropriate VLAN is automatically created if it does not yet exist.
- **Dynamically**  
VLANs can be learned through GVRP. For more information about GVRP, refer to [Section 7.1.1.8, “GARP VLAN Registration Protocol \(GVRP\)”](#)

For more information about VLANs, refer to [Section 7.1.1, “VLAN Concepts”](#).

## CONTENTS

- [Section 7.1.1, “VLAN Concepts”](#)
- [Section 7.1.2, “Viewing a List of VLANs”](#)
- [Section 7.1.3, “Configuring VLANs Globally”](#)
- [Section 7.1.4, “Configuring VLANs for Specific Ethernet Ports”](#)
- [Section 7.1.5, “Managing Static VLANs”](#)

Section 7.1.1

## VLAN Concepts

This section describes some of the concepts important to the implementation of VLANs in RUGGEDCOM ROS.

### CONTENTS

- [Section 7.1.1.1, "Tagged vs. Untagged Frames"](#)
- [Section 7.1.1.2, "Native VLAN"](#)
- [Section 7.1.1.3, "The Management VLAN"](#)
- [Section 7.1.1.4, "Edge and Trunk Port Types"](#)
- [Section 7.1.1.5, "Ingress and Egress Rules"](#)
- [Section 7.1.1.6, "Forbidden Ports List"](#)
- [Section 7.1.1.7, "VLAN-Aware and VLAN-Unaware Modes"](#)
- [Section 7.1.1.8, "GARP VLAN Registration Protocol \(GVRP\)"](#)
- [Section 7.1.1.9, "PVLAN Edge"](#)
- [Section 7.1.1.10, "QinQ"](#)
- [Section 7.1.1.11, "VLAN Advantages"](#)

Section 7.1.1.1

### Tagged vs. Untagged Frames

VLAN tags identify frames as part of a VLAN network. When a switch receives a frame with a VLAN (or 802.1Q) tag, the VLAN identifier (VID) is extracted and the frame is forwarded to other ports on the same VLAN.

When a frame does not contain a VLAN tag, or contains an 802.1p (prioritization) tag that only has prioritization information and a VID of 0, it is considered an untagged frame.

Section 7.1.1.2

### Native VLAN

Each port is assigned a native VLAN number, the Port VLAN ID (PVID). When an untagged frame ingresses a port, it is associated with the port's native VLAN.

By default, when a switch transmits a frame on the native VLAN, it sends the frame untagged. The switch can be configured to transmit tagged frames on the native VLAN.

Section 7.1.1.3

### The Management VLAN

Management traffic, like all traffic on the network, must belong to a specific VLAN. The management VLAN is configurable and always defaults to VLAN 1. This VLAN is also the default native VLAN for all ports, thus allowing all ports the possibility of managing the product. Changing the management VLAN can be used to restrict management access to a specific set of users.

## Section 7.1.1.4

## Edge and Trunk Port Types

Each port can be configured as an edge or trunk port.

An edge port attaches to a single end device, such as a PC or Intelligent Electronic Device (IED). An edge port carries traffic on the native VLAN.

Trunk ports are part of the network and carry traffic for all VLANs between switches. Trunk ports are automatically members of all VLANs configured in the switch.

The switch can 'pass through' traffic, forwarding frames received on one trunk port out of another trunk port. The trunk ports must be members of all VLANs that the 'pass through' traffic is part of, even if none of those VLANs are used on edge ports.

Frames transmitted out of the port on all VLANs other than the port's native VLAN are always sent tagged.

**NOTE**

*It may be desirable to manually restrict the traffic on the trunk to a specific group of VLANs. For example, when the trunk connects to a device, such as a Layer 3 router, that supports a subset of the available VLANs. To prevent the trunk port from being a member of the VLAN, include it in the VLAN's Forbidden Ports list.*

*For more information about the Forbidden Ports list, refer to [Section 7.1.1.6, "Forbidden Ports List"](#).*

Port Type	VLANs Supported	PVID Format	Usage
Edge	1 (Native) Configured	Untagged	<i>VLAN Unaware Networks:</i> All frames are sent and received without the need for VLAN tags.
		Tagged	<i>VLAN Aware Networks:</i> VLAN traffic domains are enforced on a single VLAN.
Trunk	All Configured	Tagged or Untagged	<i>Switch-to-Switch Connections:</i> VLANs must be manually created and administered, or can be dynamically learned through GVRP. <i>Multiple-VLAN End Devices:</i> Implement connections to end devices that support multiple VLANs at the same time.

## Section 7.1.1.5

## Ingress and Egress Rules

Ingress and egress rules determine how traffic is received and transmitted by the switch.

Ingress rules are applied as follows to all frame when they are received by the switch:

- If an incoming frame is untagged or has a VID of 0 (priority tagged), the frame is associated with the ingress port's PVID
- If an incoming frame is tagged, the frame is allowed to pass, while keeping its VID
- Incoming frames are only dropped if ingress filtering is enabled and the frame is tagged with a VID that does not match any VLAN to which the ingress port is a member

Egress rules are applied as follows to all frames when they are transmitted by the switch.

- If PVID tagging is enabled, outgoing frames are tagged if they are associated with the egress port's native VLAN, regardless of the egress port's membership type (edge or trunk)
- Frames egressing on an edge interface are dropped if they are associated with a VLAN other than the egress port's native VLAN

- Frames egressing on a trunk interface are tagged if they are associated with a VLAN to which the egress port is a member

## Section 7.1.1.6

## Forbidden Ports List

Each VLAN can be configured to exclude ports from membership in the VLAN using the forbidden ports list. For more information, refer to [Section 7.1.5.2, "Adding a Static VLAN"](#).

## Section 7.1.1.7

## VLAN-Aware and VLAN-Unaware Modes

The native operation mode for an IEEE 802.1Q compliant switch is VLAN-aware. Even if a specific network architecture does not use VLANs, RUGGEDCOM ROS's default VLAN settings allow the switch to still operate in a VLAN-aware mode, while providing functionality required for almost any network application. However, the IEEE 802.1Q standard defines a set of rules that must be followed by all VLAN-aware switches:

- Valid VIDs are within the range of 1 to 4094. VID equal to 0 or 4095 are invalid.
- Each frame ingressing a VLAN-aware switch is associated with a valid VID.
- Each frame egressing a VLAN-aware switch is either untagged or tagged with a valid VID. Priority-tagged frames with an invalid VID will never sent out by a VLAN-aware switch.

**NOTE**

*Some applications have requirements conflicting with IEEE 802.Q1 native mode of operation. For example, some applications explicitly require priority-tagged frames to be received by end devices.*

*To avoid conflicts and provide full compatibility with legacy (VLAN-unaware) devices, RUGGEDCOM ROS can be configured to work in VLAN-unaware mode.*

*In that mode:*

- *Frames ingressing a VLAN-unaware device are not associated with any VLAN*
- *Frames egressing a VLAN-unaware device are sent out unmodified (i.e. in the same untagged, 802.1Q-tagged or priority-tagged format as they were received)*

## Section 7.1.1.8

## GARP VLAN Registration Protocol (GVRP)

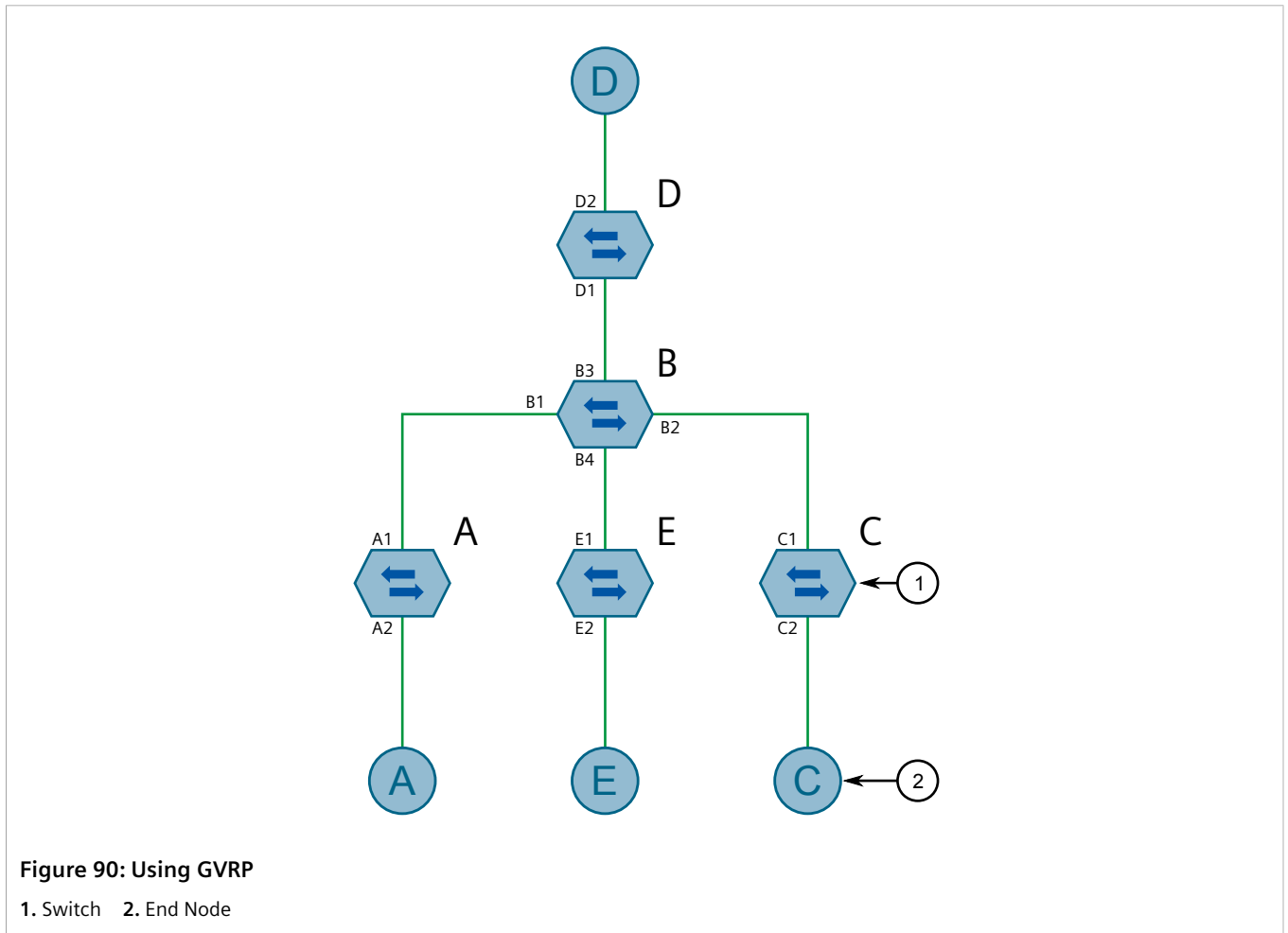
GARP VLAN Registration Protocol (GVRP) is a standard protocol built on GARP (Generic Attribute Registration Protocol) to automatically distribute VLAN configuration information in a network. Each switch in a network needs only to be configured with VLANs it requires locally. VLANs configured elsewhere in the network are learned through GVRP. A GVRP-aware end station (i.e. PC or Intelligent Electronic Device) configured for a particular VID can be connected to a trunk on a GVRP-aware switch and automatically become part of the desired VLAN.

When a switch sends GVRP bridge protocol data units (BPDUs) out of all GVRP-enabled ports, GVRP BPDUs advertise all the VLANs known to that switch (configured manually or learned dynamically through GVRP) to the rest of the network.

When a GVRP-enabled switch receives a GVRP BPDU advertising a set of VLANs, the receiving port becomes a member of those advertised VLANs and the switch begins advertising those VLANs through all the GVRP-enabled ports (other than the port on which the VLANs were learned).

To improve network security using VLANs, GVRP-enabled ports may be configured to prohibit the learning of any new dynamic VLANs but at the same time be allowed to advertise the VLANs configured on the switch.

The following is an example of how to use GVRP:



- Switch B is the core switch, all others are edge switches
- Ports A1, B1 to B4, C1, D1, D2 and E1 are GVRP aware
- Ports B1 to B4, D1 and D2 are set to advertise and learn
- Ports A1, C1 and E1 are set to advertise only
- Ports A2, C2 and E2 are edge ports
- End node D is GVRP aware
- End nodes A, E and C are GVRP unaware
- Ports A2 and C2 are configured with PVID 7
- Port E2 is configured with PVID 20
- End node D is interested in VLAN 20, hence VLAN 20 is advertised by it towards switch D
- D2 becomes a member of VLAN 20
- Ports A1 and C1 advertise VID 7
- Ports B1 and B2 become members of VLAN 7

- Ports B1, B2 and D1 advertise VID 20
- Ports B3, B4 and D1 become members of VLAN 20

For more information about how to configure GVRP, refer to [Section 7.1.4, “Configuring VLANs for Specific Ethernet Ports”](#).

#### Section 7.1.1.9

### PVLAN Edge

Private VLAN (PVLAN) Edge isolates multiple VLAN Edge ports from each other on a single device. When VLAN Edge ports are configured as *protected*, they are prohibited from sending frames to one another, but are still permitted to send frames to other, non-protected ports within the same VLAN. This protection extends to all traffic on the VLAN, including unicast, multicast and broadcast traffic.

For more information about how to configure a port as *protected*, refer to [Section 7.1.4, “Configuring VLANs for Specific Ethernet Ports”](#).



#### NOTE

*This feature is strictly local to the switch. PVLAN Edge ports are not prevented from communicating with ports outside of the switch, whether protected (remotely) or not.*

#### Section 7.1.1.10

### QinQ

QinQ, also referred to as Stacked VLANs, port bridging, double VLAN-tagging and Nested VLANs, is used to overlay a private Layer 2 network over a public Layer 2 network.

A large network service provider, for example, might have several clients whose networks each use multiple VLANs. It is likely the VLAN IDs used by these different client networks would conflict with one another, were they mixed together in the provider's network. Using double QinQ, each client network could be further tagged using a client-specific VID at the edges where the clients' networks are connected to the network service provider's infrastructure.

Any tagged frames ingressing an edge port of the service provider's switch are tagged with VIDs of the customer's private network. When those frames egress the switch's QinQ-enabled port into the service provider network, the switch always adds an extra tag (called an *outer tag*) on top of the frame's original VLAN tag (called an *inner tag*). The outer tag VID is the PVID of the frame's ingress edge port. This means that traffic from an individual customer is tagged with their unique VID and is thus segregated from other customers' traffic. For untagged ingress frames, the switch will only add the outer VLAN tag.

Within the service provider network, switching is based on the VID in the outer tag.

The service provider strips the outer VID from the frame on egress, leaving the frame with its original VLAN ID tag. Those frames are then forwarded on the appropriate VLANs.

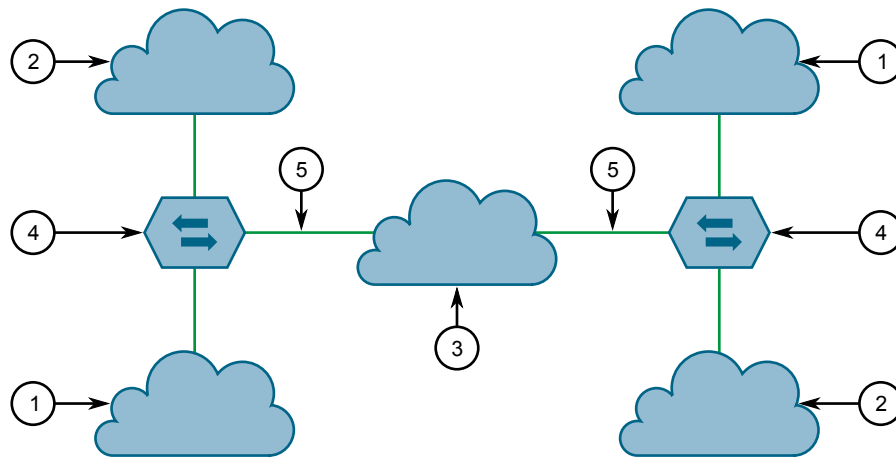
The following figure shows an example of traffic flow using QinQ.

For tagged frames:

- Frames received from customer 1 with VID 100 would carry an inner tag of 100 and an outer tag of VID X (i.e. VLAN 110) which is configured on the edge port connected to customer 1.
- Next, the frames from customer 1 are forwarded through the QinQ port carrying an inner and an outer tag.
- Finally, upon arrival of the frames in the peer switch, the outer VLAN tag is removed and the frames are forwarded with the inner VLAN tag towards customer 1.

For untagged frames:

- Frames received from customer 2 would carry an outer tag of VID Y(i.e VLAN 220) which is configured on the edge port connected to customer 2.
- Next, the frames from customer 2 are forwarded through the QinQ port carrying the outer tag.
- Finally, upon arrival of the frames in the peer switch, the outer VLAN tag is removed before the frames are forwarded to customer 2.



**Figure 91: Using QinQ**

1. Customer 1 (PVID is X) 2. Customer 2 (PVID is Y) 3. Network Service Provider Infrastructure 4. Switch 5. QinQ



**NOTE**

Depending on the hardware installed, some switch models allow only one switch port be configured to QinQ mode at a time.



**NOTE**

When QinQ is enabled, all non-QinQ ports will be untagged and cannot be changed, and all QinQ ports will be tagged, and cannot be changed.

Section 7.1.1.11

## VLAN Advantages

The following are a few of the advantages offered by VLANs.

### » Traffic Domain Isolation

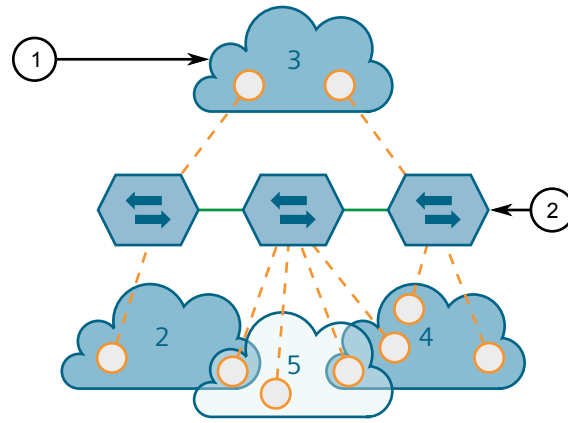
VLANs are most often used for their ability to restrict traffic flows between groups of devices.

Unnecessary broadcast traffic can be restricted to the VLAN that requires it. Broadcast storms in one VLAN need not affect users in other VLANs.

Hosts on one VLAN can be prevented from accidentally or deliberately assuming the IP address of a host on another VLAN.

The use of creative bridge filtering and multiple VLANs can carve seemingly unified IP subnets into multiple regions policed by different security/access policies.

Multi-VLAN hosts can assign different traffic types to different VLANs.



**Figure 92: Multiple Overlapping VLANs**

1. VLAN 2. Switch

### » Administrative Convenience

VLANs enable equipment moves to be handled by software reconfiguration instead of by physical cable management. When a host's physical location is changed, its connection point is often changed as well. With VLANs, the host's VLAN membership and priority are simply copied to the new port.

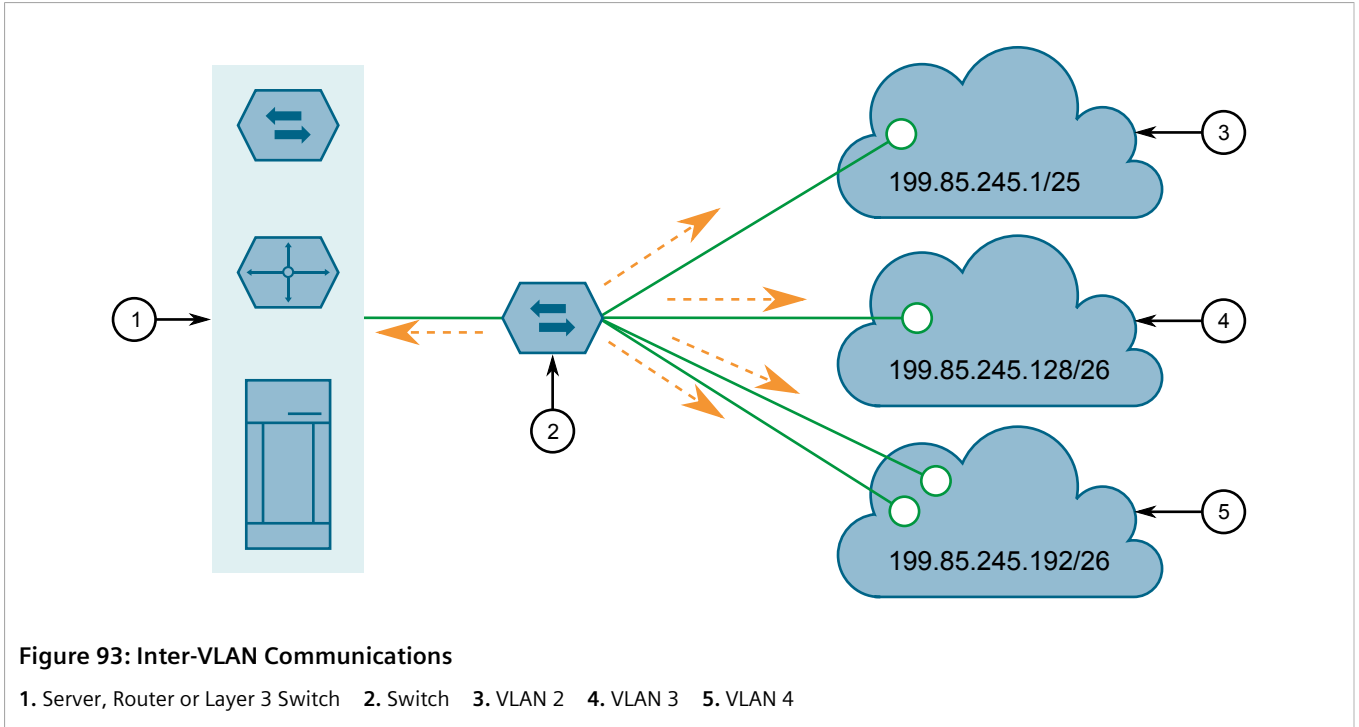
### » Reduced Hardware

Without VLANs, traffic domain isolation requires the use of separate bridges for separate networks. VLANs eliminate the need for separate bridges.

The number of network hosts may often be reduced. Often, a server is assigned to provide services for independent networks. These hosts may be replaced by a single, multi-horned host supporting each network on its own VLAN. This host can perform routing between VLANs.

Multi-VLAN hosts can assign different traffic types to different VLANs.

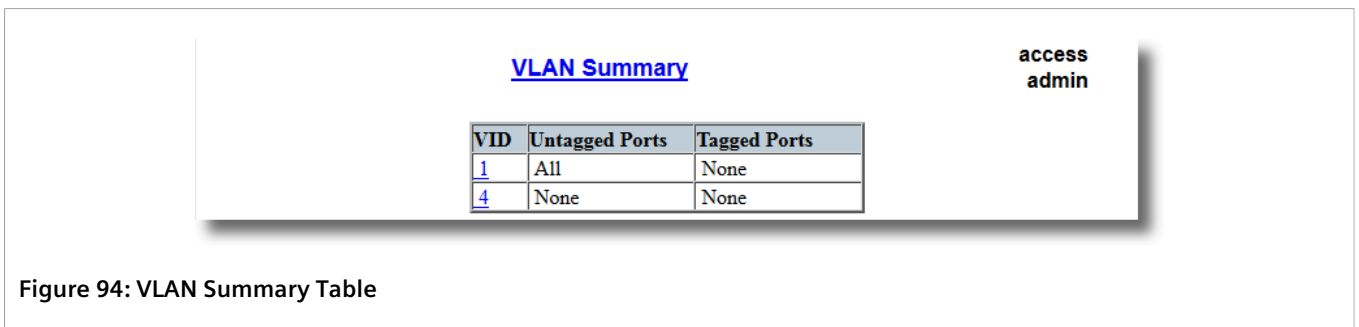




Section 7.1.2

## Viewing a List of VLANs

To view a list of all VLANs, whether they were created statically, implicitly or dynamically, navigate to **Virtual LANs » View VLAN Summary**. The **VLAN Summary** table appears.



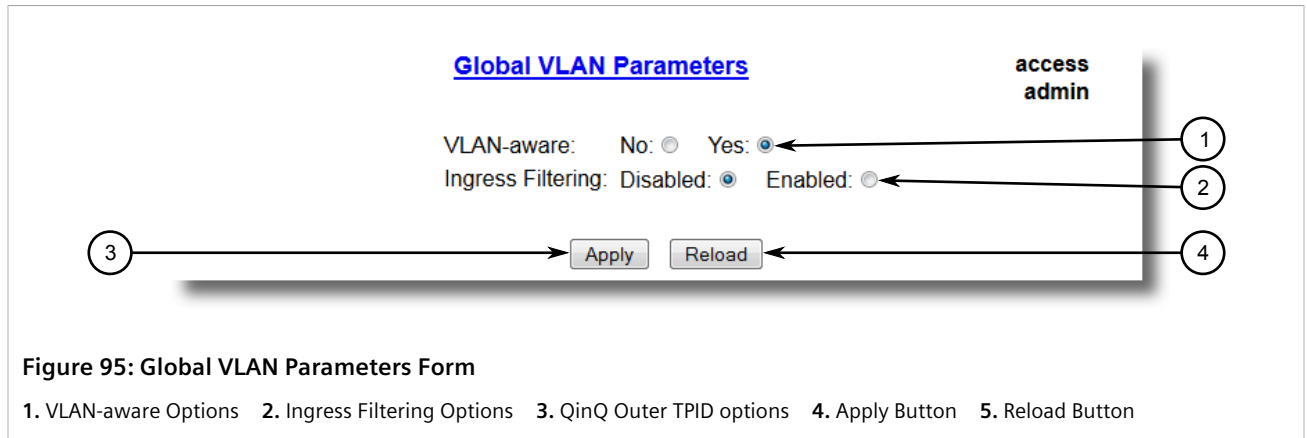
If a VLANs are not listed, add static VLANs as needed. For more information, refer to [Section 7.1.5.2, “Adding a Static VLAN”](#).

Section 7.1.3

## Configuring VLANs Globally

To configure global settings for all VLANs, do the following:

1. Navigate to **Virtual LANs » Configure Global VLAN Parameters**. The **Global VLAN Parameters** form appears.



**Figure 95: Global VLAN Parameters Form**

1. VLAN-aware Options   2. Ingress Filtering Options   3. QinQ Outer TPID options   4. Apply Button   5. Reload Button

2. Configure the following parameter(s) as required:

Parameter	Description
VLAN-aware	<p><b>Synopsis:</b> { No, Yes }</p> <p><b>Default:</b> Yes</p> <p>Set either VLAN-aware or VLAN-unaware mode of operation.</p>
Ingress Filtering	<p><b>Synopsis:</b> { Disabled, Enabled }</p> <p><b>Default:</b> Disabled</p> <p>Enables or disables VLAN ingress filtering on all ports. When enabled, any tagged packet arriving at a port, which is not a member of a VLAN with which that packet is associated, is dropped. When disabled, packets are not dropped.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p><b>NOTE</b> Ingress filtering has no effect when ports are in either VLAN-unaware mode or Q-in-Q mode.</p> </div>

3. Click **Apply**.

Section 7.1.4

## Configuring VLANs for Specific Ethernet Ports

When a VLAN ID is assigned to an Ethernet port, the VLAN appears in the VLAN Summary table where it can be further configured.

To configure a VLAN for a specific Ethernet port, do the following:

1. Navigate to **Virtual LANs » Configure Port VLAN Parameters**. The **Port VLAN Parameters** table appears.

**Port VLAN Parameters**

Port(s)	Type	PVID	PVID Format	GVRP
<a href="#">1</a>	Edge	1	Untagged	Disabled
<a href="#">2</a>	Edge	1	Untagged	Disabled
<a href="#">3</a>	Edge	1	Untagged	Disabled
<a href="#">4</a>	Edge	1	Untagged	Disabled
<a href="#">5</a>	Edge	1	Untagged	Disabled
<a href="#">6</a>	Edge	1	Untagged	Disabled
<a href="#">7</a>	Edge	1	Untagged	Disabled
<a href="#">8</a>	Edge	1	Untagged	Disabled
<a href="#">9</a>	Edge	1	Untagged	Disabled
<a href="#">10</a>	Edge	1	Untagged	Disabled

**access  
admin**

**Figure 96: Port VLAN Parameters Table**

- Select a port. The **Port VLAN Parameters** form appears.

**Port VLAN Parameters**

**access  
admin**

Port(s):  ← 1

Type:  ← 2

PVID:  ← 3

PVID Format: Untagged:  Tagged:  ← 4

GVRP:  ← 5


← 6  ← 7

**Figure 97: Port VLAN Parameters Form**

1. Port(s) Box 2. Type List 3. PVID Box 4. PVID Format Options 5. GVRP List 6. Apply Button 7. Reload Button

- Configure the following parameter(s) as required:

Parameter	Description
Port(s)	<b>Synopsis:</b> Any combination of numbers valid for this parameter The port number as seen on the front plate silkscreen of the switch (or a list of ports, if aggregated in a port trunk).
Type	<b>Synopsis:</b> { Edge, Trunk, PVLANEdge, QinQ } <b>Default:</b> Edge This parameter specifies how the port determines its membership in VLANs. There are few types of ports: <ul style="list-style-type: none"> <li>Edge - the port is only a member of one VLAN (its native VLAN specified by the <i>PVID</i> parameter).</li> <li>Trunk - the port is automatically a member of all configured VLANs. Frames transmitted out of the port on all VLANs except the port's native VLAN will be always tagged. It can also be configured to use GVRP for automatic VLAN configuration.</li> </ul>

Parameter	Description
	<ul style="list-style-type: none"> <li>PVLANEdge - the port is only a member of one VLAN (its native VLAN specified by the <i>PVID</i> parameter), and does not forward traffic to other PVLANEdge ports within the same VLAN.</li> <li>QinQ - the port is a trunk port using double-VLAN tagging, or nested VLANs. An extra VLAN tag is always added to all frames egressing this port. VID in the added extra tag is the PVID of the frame's ingress port. VLAN tag is always stripped from frames ingressing this port.</li> </ul> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;">  <b>NOTE</b>  <i>QinQ can only be enabled on one switch port at a time.</i> </div>
PVID	<p><b>Synopsis:</b> 1 to 4094 <b>Default:</b> 1</p> <p>The Port VLAN Identifier specifies the VLAN ID associated with untagged (and 802.1p priority tagged) frames received on this port.</p> <p>Frames tagged with a non-zero VLAN ID will always be associated with the VLAN ID retrieved from the frame tag.</p> <p>Modify this parameter with care! By default, the switch is programmed to use VLAN 1 for management and every port on the switch is programmed to use VLAN 1. If you modify a switch port to use a VLAN other than the management VLAN, devices on that port will not be able to manage the switch.</p>
PVID Format	<p><b>Synopsis:</b> { Untagged, Tagged } <b>Default:</b> Untagged</p> <p>Specifies whether frames transmitted out of the port on its native VLAN (specified by the <i>PVID</i> parameter) will be tagged or untagged.</p> <p>If <i>Type</i> is set to <i>QinQ</i>, set the PVID format to <i>Tagged</i> and make sure all other ports are set to <i>Untagged</i>.</p>
GVRP	<p><b>Synopsis:</b> { Adv&amp;Learn, Adv Only, Disabled } <b>Default:</b> Disabled</p> <p>Configures GVRP (Generic VLAN Registration Protocol) operation on the port. There are several GVRP operation modes:</p> <ul style="list-style-type: none"> <li>DISABLED - the port is not capable of any GVRP processing.</li> <li>ADVERTISE ONLY - the port will declare all VLANs existing in the switch (configured or learned) but will not learn any VLANs.</li> <li>ADVERTISE &amp; LEARN - the port will declare all VLANs existing in the switch (configured or learned) and can dynamically learn VLANs.</li> </ul> <p>Only Trunk ports are GVRP-capable.</p>

- Click **Apply**.

## Section 7.1.5

## Managing Static VLANs

This section describes how to configure and manage static VLANs.

### CONTENTS

- [Section 7.1.5.1, "Viewing a List of Static VLANs"](#)
- [Section 7.1.5.2, "Adding a Static VLAN"](#)
- [Section 7.1.5.3, "Deleting a Static VLAN"](#)

Section 7.1.5.1

## Viewing a List of Static VLANs

To view a list of static VLANs, navigate to *Virtual LANs » Configure Static VLANs*. The **Static VLANs** table appears.

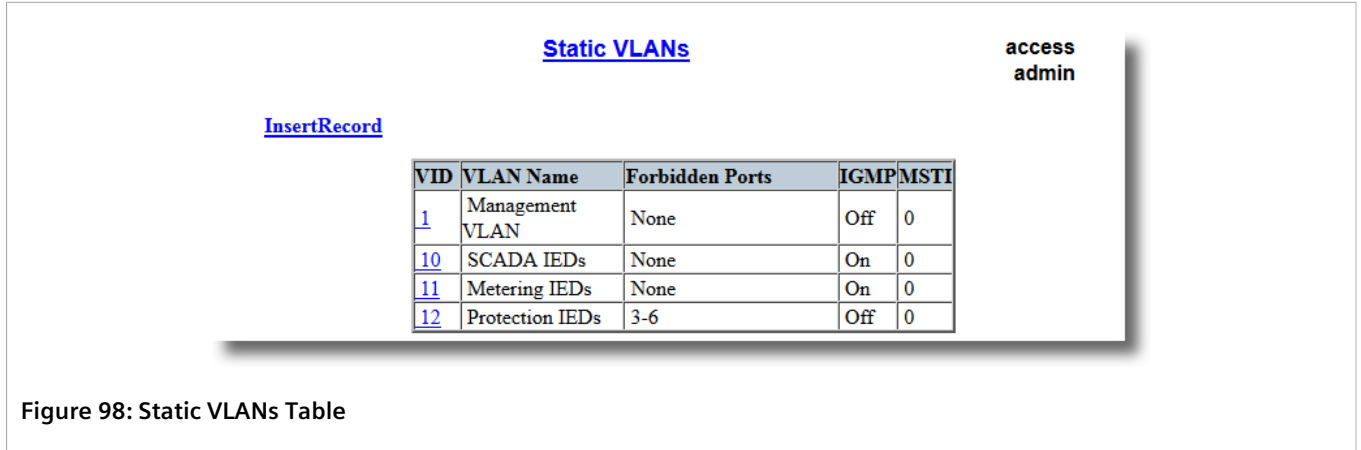


Figure 98: Static VLANs Table

If a static VLAN is not listed, add the VLAN. For more information, refer to [Section 7.1.5.2, “Adding a Static VLAN”](#).

Section 7.1.5.2

## Adding a Static VLAN

To add a static VLAN, do the following:

1. Navigate to *Virtual LANs » Configure Static VLANs*. The **Static VLANs** table appears.

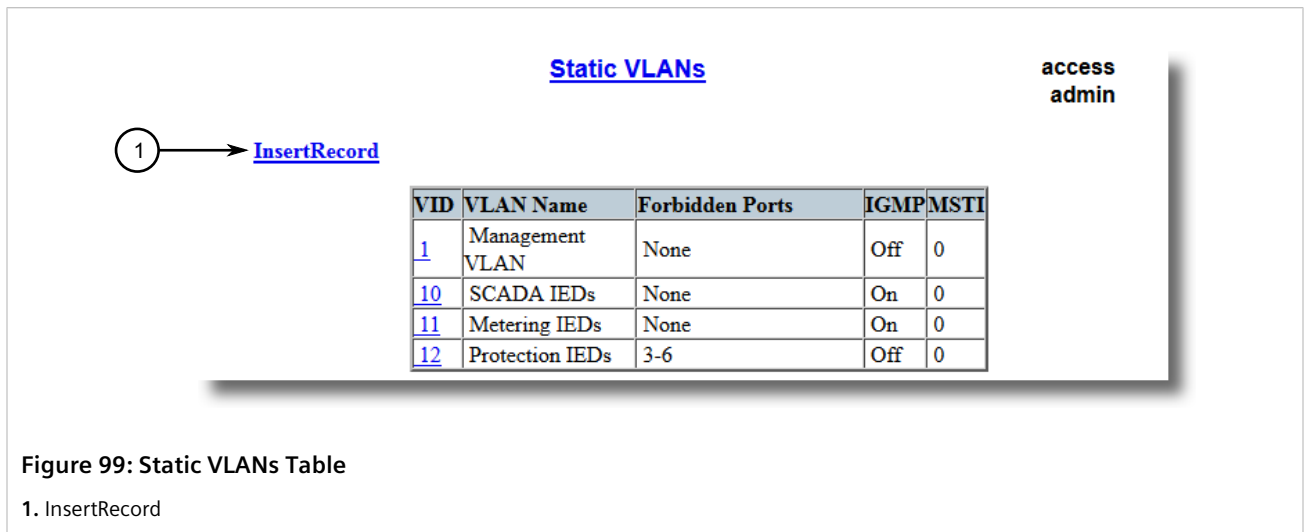
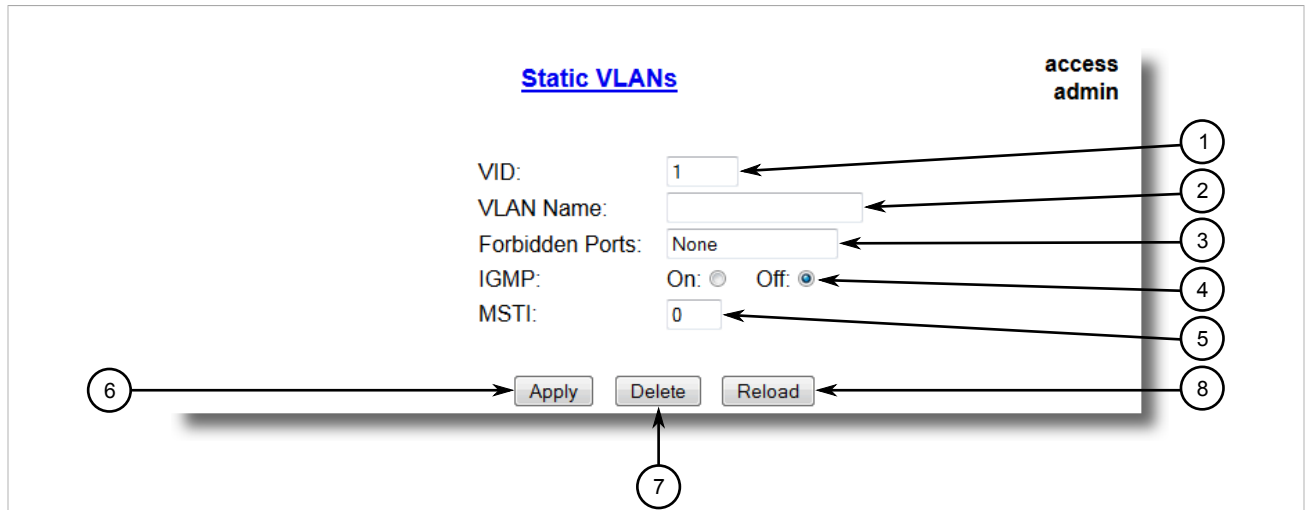


Figure 99: Static VLANs Table

1. InsertRecord

2. Click **InsertRecord**. The **Static VLANs** form appears.



**Figure 100: Static VLANs Form**

1. VID Box 2. VLAN Name Box 3. Forbidden Ports Box 4. IGMP Options 5. MSTI Box 6. Apply Button 7. Delete Button 8. Reload Button

3. Configure the following parameter(s) as required:



**NOTE**

*If IGMP Options is not enabled for the VLAN, both IGMP messages and multicast streams will be forwarded directly to all members of the VLAN. If any one member of the VLAN joins a multicast group, then all members of the VLAN will receive the multicast traffic.*

Parameter	Description
VID	<p><b>Synopsis:</b> 1 to 4094  <b>Synopsis:</b> 1 to 4094  <b>Default:</b> 1</p> <p>The VLAN Identifier is used to identify the VLAN in tagged Ethernet frames according to IEEE 802.1Q.</p>
VLAN Name	<p><b>Synopsis:</b> Any 19 characters</p> <p>The VLAN name provides a description of the VLAN purpose (for example, Engineering VLAN).</p>
Forbidden Ports	<p><b>Synopsis:</b> Any combination of numbers valid for this parameter</p> <p>These are ports that are not allowed to be members of the VLAN.</p> <p>Examples:</p> <ul style="list-style-type: none"> <li>• None - all ports of the switch are allowed to be members of the VLAN</li> <li>• 2,4-6,8 - all ports except ports 2, 4, 6, 7 and 8 are allowed to be members of the VLAN</li> </ul>
IGMP	<p><b>Synopsis:</b> { Off, On }  <b>Default:</b> Off</p> <p>This parameter enables or disables IGMP Snooping on the VLAN.</p>
MSTI	<p><b>Synopsis:</b> 0 to 16  <b>Default:</b> 0</p> <p>This parameter is only valid for Multiple Spanning Tree Protocol (MSTP) and has no effect if MSTP is not used. The parameter specifies the Multiple Spanning Tree Instance (MSTI) to which the VLAN should be mapped.</p>

4. Click **Apply**.

Section 7.1.5.3

## Deleting a Static VLAN

To delete a static VLAN, do the following:

1. Navigate to **Virtual LANs » Configure Static VLANs**. The **Static VLANs** table appears.

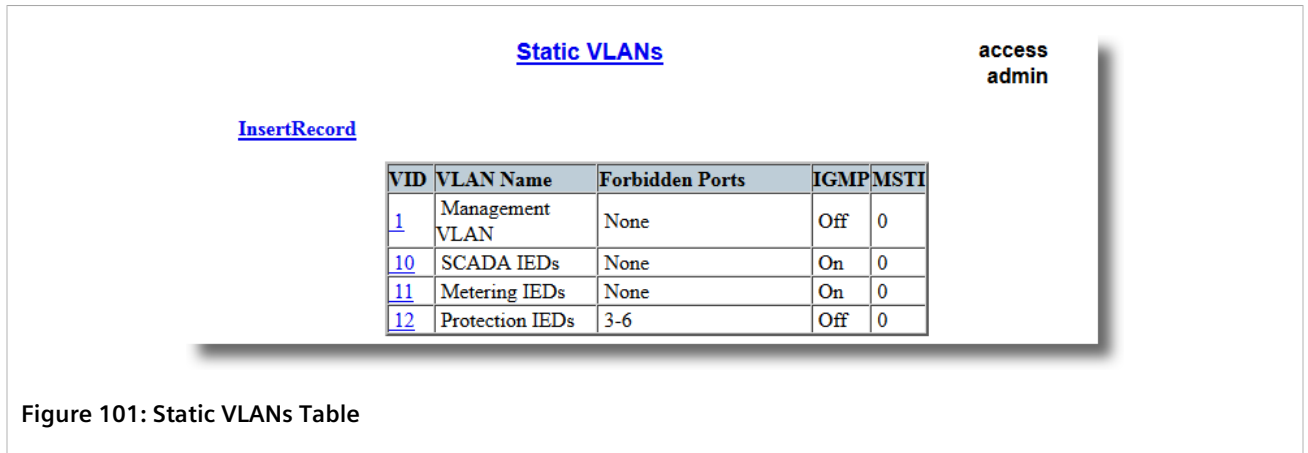


Figure 101: Static VLANs Table

2. Select the static VLAN from the table. The **Static VLANs** form appears.

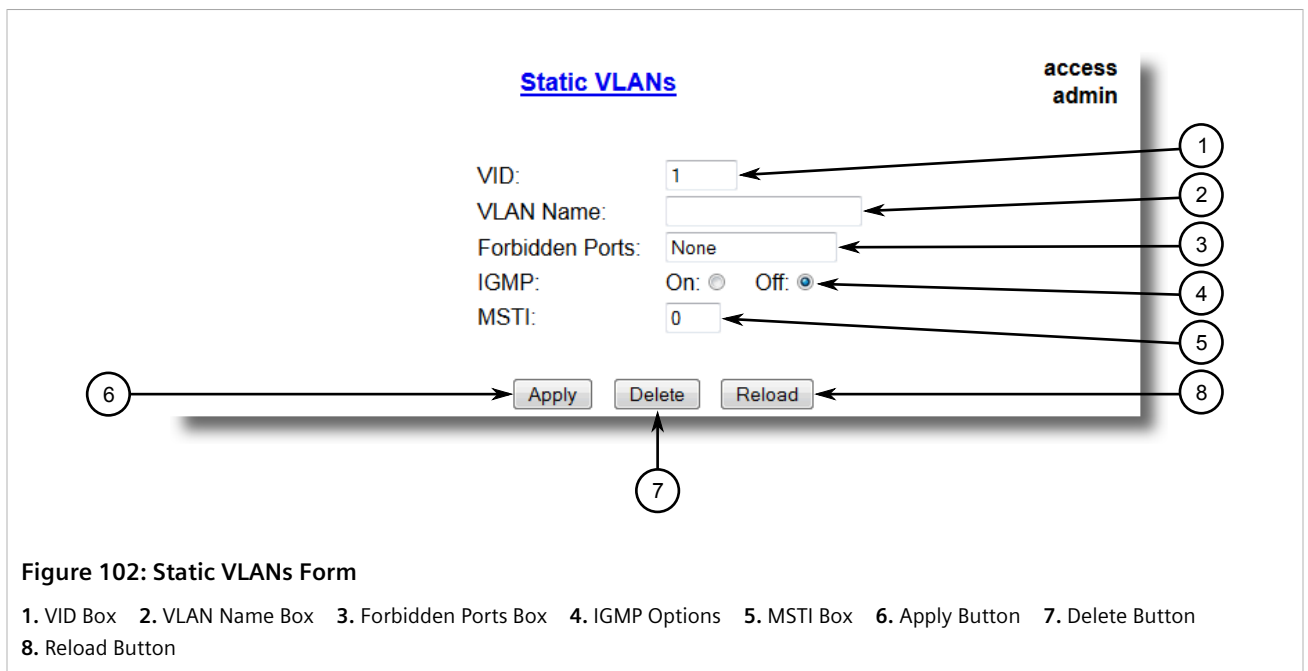


Figure 102: Static VLANs Form

1. VID Box
2. VLAN Name Box
3. Forbidden Ports Box
4. IGMP Options
5. MSTI Box
6. Apply Button
7. Delete Button
8. Reload Button

3. Click **Delete**.

Section 7.2

# Managing MAC Addresses

This section describes how to manage MAC addresses.

## CONTENTS

- [Section 7.2.1, “Viewing a List of MAC Addresses”](#)
- [Section 7.2.2, “Configuring MAC Address Learning Options”](#)
- [Section 7.2.3, “Configuring MAC Address Flooding Options”](#)
- [Section 7.2.4, “Managing Static MAC Addresses”](#)
- [Section 7.2.5, “Purging All Dynamic MAC Addresses”](#)

Section 7.2.1

## Viewing a List of MAC Addresses

To view a list of all static and dynamically learned MAC addresses, navigate to **MAC Address Tables » View MAC Addresses**. The **MAC Addresses** table appears.



<b>MAC Addresses</b>					access admin
MAC Address	VID	Port	Type	CoS	
<a href="#">00-01-6C-4A-60-1A</a>	1	8	Dynamic	N/A	
<a href="#">00-01-C0-0B-B8-42</a>	1	8	Dynamic	N/A	
<a href="#">00-01-C0-0C-0B-B7</a>	1	8	Dynamic	N/A	
<a href="#">00-06-B5-64-92-75</a>	1	8	Dynamic	N/A	
<a href="#">00-0A-DC-00-1E-CA</a>	1	8	Dynamic	N/A	
<a href="#">00-0A-DC-11-33-40</a>	1	8	Dynamic	N/A	
<a href="#">00-0A-DC-2D-A6-E3</a>	1	8	Dynamic	N/A	
<a href="#">00-0A-DC-E5-86-FF</a>	1	8	Dynamic	N/A	
<a href="#">00-0A-DC-E5-A4-FF</a>	1	8	Dynamic	N/A	
<a href="#">00-0A-DC-F1-7A-FF</a>	1	8	Dynamic	N/A	
<a href="#">00-0A-DC-F1-7B-FF</a>	1	8	Dynamic	N/A	
<a href="#">00-0A-DC-F1-84-FD</a>	1	8	Dynamic	N/A	
<a href="#">00-0A-DC-F1-8C-FD</a>	1	8	Dynamic	N/A	
<a href="#">00-0A-DC-F1-D7-FF</a>	1	8	Dynamic	N/A	
<a href="#">00-0A-DC-F3-5D-FF</a>	1	8	Dynamic	N/A	

Figure 103: MAC Address Table

If a MAC address is not listed, do the following:

1. Configure the MAC address learning options to control the aging time of dynamically learned MAC addresses of other devices on the network. For more information, refer to [Section 7.2.2, "Configuring MAC Address Learning Options"](#).
2. Configure the address on the device as a static MAC address. For more information, refer to [Section 7.2.4.2, "Adding a Static MAC Address"](#).

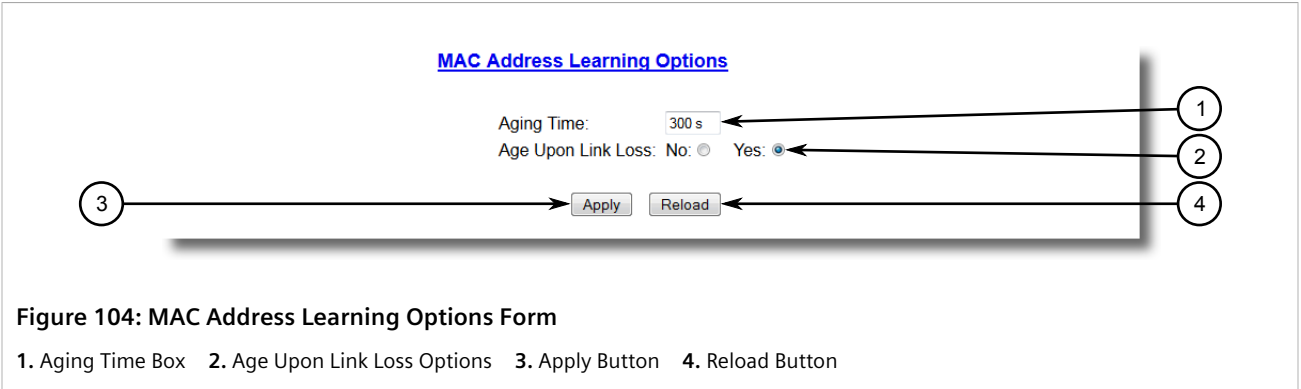
## Section 7.2.2

## Configuring MAC Address Learning Options

The MAC address learning options control how and when MAC addresses are removed automatically from the MAC address table. Individual addressees are removed when the aging timer is exceeded. Addresses can also be removed when a link failure or topology change occurs.

To configure the MAC address learning options, do the following:

1. Navigate to **MAC Address Tables » Configure MAC Address Learning Options**. The **MAC Address Learning Options** form appears.



2. Configure the following parameter(s) as required:

Parameter	Description
Aging Time	<p><b>Synopsis:</b> 15 to 800 <b>Default:</b> 300 s</p> <p>This parameter configures the time that a learned MAC address is held before being aged out.</p>
Age Upon Link Loss	<p><b>Synopsis:</b> { No, Yes } <b>Default:</b> Yes</p> <p>When set to Yes, all MAC addresses learned on a failed port will be aged-out immediately upon link failure detection.</p> <p>When link failure occurs the switch may have some MAC addresses previously learned on the failed port. As long as those addresses are not aged-out the switch will still be forwarding traffic to that port, thus preventing that traffic from reaching its destination via the new network topology.</p> <p>Note that when a network redundancy protocol, e.g. RSTP/MSTP, is enabled on the switch, that redundancy protocol may, upon a link failure, flush MAC addresses learned on the failed port regardless of the setting of this parameter.</p>

3. Click **Apply**.

Section 7.2.3

## Configuring MAC Address Flooding Options

To configure the MAC address flooding options, do the following:

1. Navigate to **MAC Address Tables » Configure MAC Address Flooding Options**. The **Flooding Options** table appears.

**Flooding Options**

**access  
admin**

Port(s)	Flood Unknown Unicast
<a href="#">1</a>	On
<a href="#">2</a>	On
<a href="#">3</a>	On
<a href="#">4</a>	On
<a href="#">5</a>	On
<a href="#">6</a>	On
<a href="#">7</a>	On
<a href="#">8</a>	On
<a href="#">9</a>	On
<a href="#">10</a>	On

**Figure 105: Flooding Options Table**

- Select a port. The **Flooding Options** form appears.

**Flooding Options**

**access  
admin**

Port(s):  ← 1

Flood Unknown Unicast: On:  Off:  ← 2

← 3      ← 4

**Figure 106: Flooding Options Form**

1. Port(s) Box   2. Flood Unknown Unicast Options   3. Apply Button   4. Reload Button

- Configure the following parameter(s) as required:

Parameter	Description
Port(s)	<b>Synopsis:</b> Comma-separated list of ports The port number as seen on the front plate silkscreen of the switch (or a list of ports, if aggregated in a port trunk).
Flood Unknown Unicast	<b>Synopsis:</b> { On, Off } <b>Default:</b> On Normally, unicast traffic with an unknown destination address is flooded out of all ports. When a port is configured to turn off this kind of flooding, the unknown unicast traffic is not sent out from the selected port.

- Click **Apply**.

## Section 7.2.4

## Managing Static MAC Addresses

Static MAC addresses must be configured when the device is only able to receive frames, not transmit them. They may also need to be configured if port security (if supported) must be enforced.

Prioritized MAC addresses are configured when traffic to or from a specific device on a LAN segment is to be assigned a higher CoS priority than other devices on that LAN segment.

**NOTE**

A MAC address cannot be learned on a VLAN that has not been configured in the Static VLAN table. If a frame with an unknown VLAN tag arrives on a secured port, it is considered a security violation and RUGGEDCOM ROS will generate a port security alarm.

**CONTENTS**

- [Section 7.2.4.1, “Viewing a List of Static MAC Addresses”](#)
- [Section 7.2.4.2, “Adding a Static MAC Address”](#)
- [Section 7.2.4.3, “Deleting a Static MAC Address”](#)

## Section 7.2.4.1

### Viewing a List of Static MAC Addresses

To view a list of static MAC addresses configured on the device, navigate to **MAC Address Tables » Configure Static MAC Addresses**. The **Static MAC Addresses** table appears.

MAC Address	VID	Port	CoS
<a href="#">00-00-00-00-00-01</a>	1	1	High
<a href="#">00-00-00-00-00-02</a>	1	2	Medium
<a href="#">00-00-00-00-00-03</a>	1	3	Normal

Figure 107: Static MAC Address Table

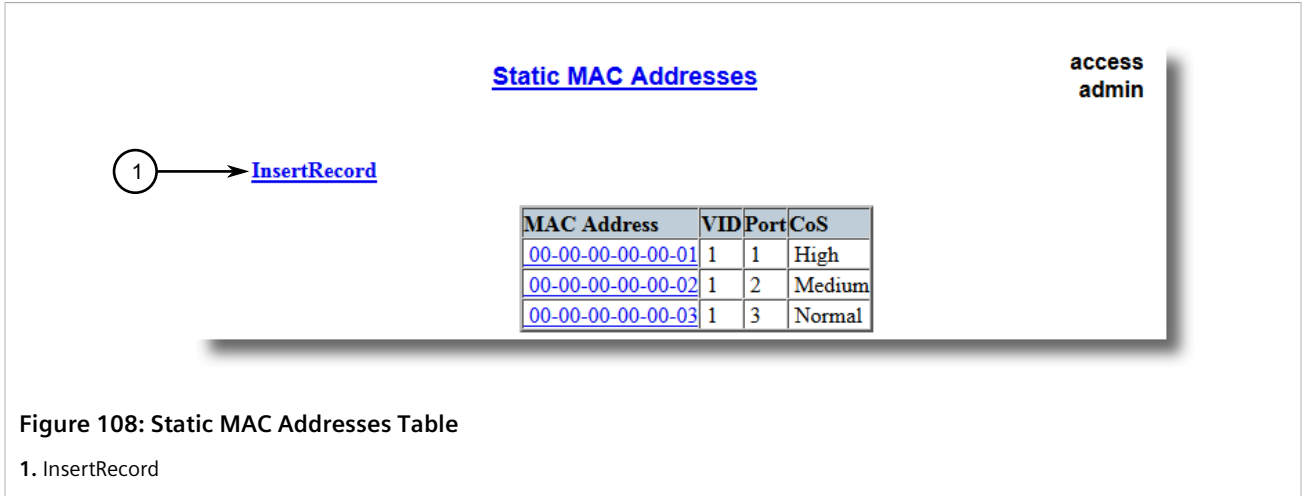
If static MAC addresses have not been configured, add addresses as needed. For more information, refer to [Section 7.2.4.2, “Adding a Static MAC Address”](#).

## Section 7.2.4.2

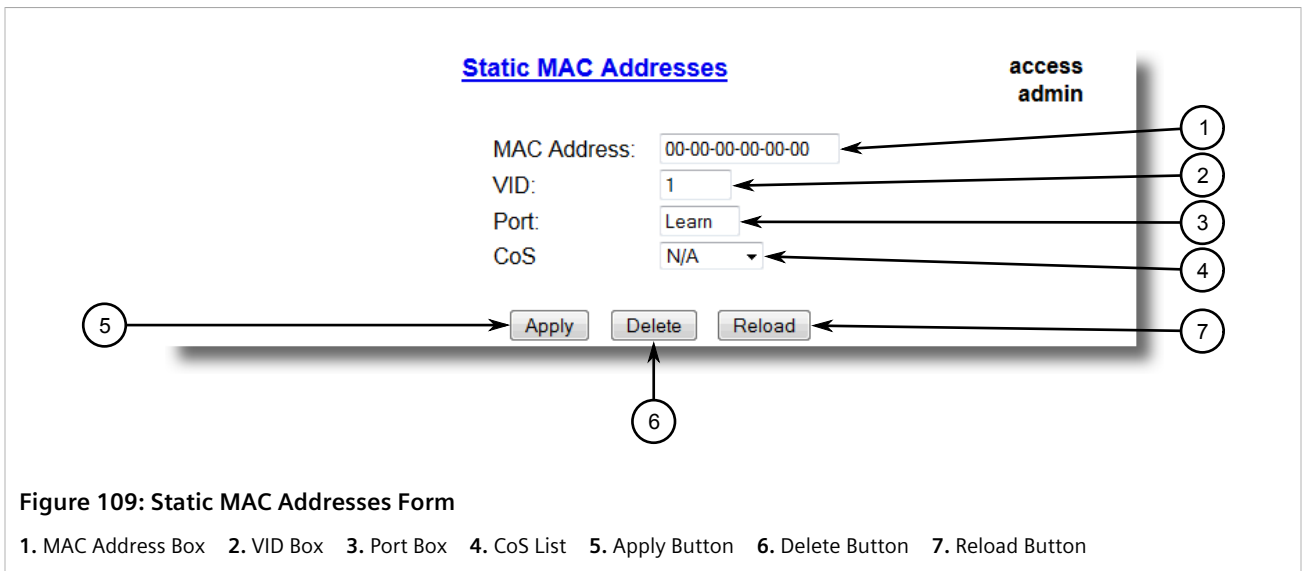
### Adding a Static MAC Address

To add a static MAC address to the Static MAC Address Table, do the following:

1. Navigate to **MAC Address Tables » Configure Static MAC Addresses**. The **Static MAC Addresses** table appears.



- Click **InsertRecord**. The **Static MAC Addresses** form appears.



- Configure the following parameter(s) as required:

Parameter	Description
MAC Address	<p><b>Synopsis:</b> ##-##-##-##-##-## where ## ranges 0 to FF</p> <p>A MAC address learned by the switch.</p> <p>Maximum of 6 wildcard characters may be used to specify a range of MAC addresses allowed to be learned by the Port Security module (when Port Security is set to 'Static MAC' mode). Wildcard must start from the right hand end and continuous.</p> <p>Examples:</p> <ul style="list-style-type: none"> <li>00-0A-DC-**-**-** means the entire MAC address space of RuggedCom.</li> <li>00-0A-DC-12-3**-** means the range 00-0A-DC-12-30-00 to 00-0A-DC-12-3F-FF.</li> </ul>
VID	<p><b>Synopsis:</b> 1 to 4094 or { ANY }</p> <p><b>Default:</b> 1</p> <p>VLAN Identifier of the VLAN upon which the MAC address operates.</p> <p>Option ANY allows learning a MAC address through the Port Security module on any VLAN's that are configured on the switch.</p>

Parameter	Description
Port	<p><b>Synopsis:</b> 1 to maximum port number or { Learn }</p> <p><b>Default:</b> Learn</p> <p>Enter the port number upon which the device with this address is located. The security mode of the port being selected should not be '802.1X'.</p> <p>If the port should be auto-learned, set this parameter to 'Learn'. The option 'Learn' is applicable for Port Security in 'Static MAC' mode.</p>
CoS	<p><b>Synopsis:</b> { N/A, Normal, Medium, High, Crit }</p> <p><b>Default:</b> N/A</p> <p>Prioritizes traffic for the specified MAC address. To not prioritize traffic based on the address, select N/A.</p>

- Click **Apply**.

### Section 7.2.4.3

## Deleting a Static MAC Address

To delete a static MAC address from the Static MAC Address Table, do the following:

- Navigate to **MAC Address Tables » Configure Static MAC Addresses**. The **Static MAC Addresses** table appears.

**Static MAC Addresses**

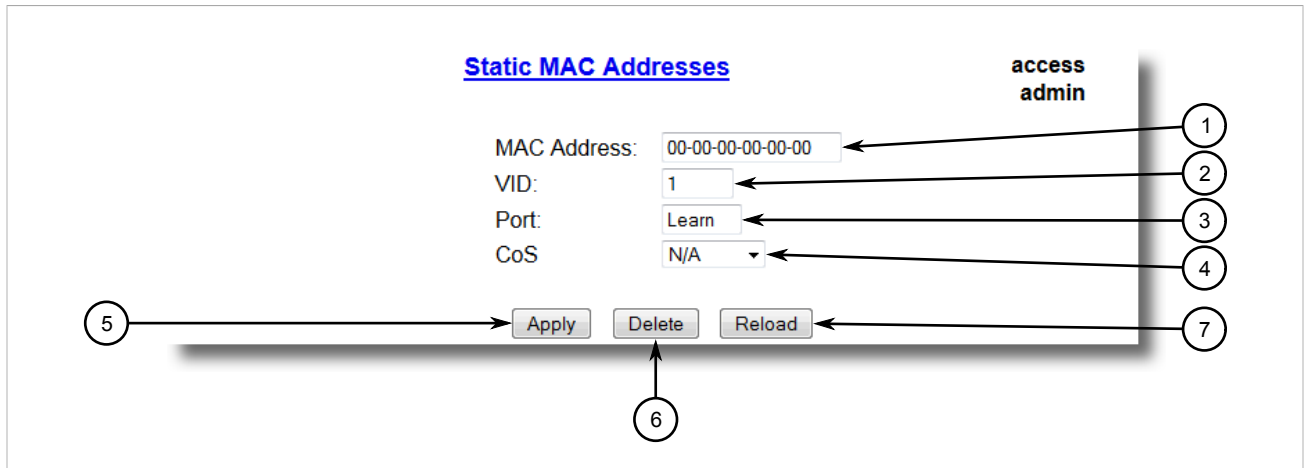
access  
admin

[InsertRecord](#)

MAC Address	VID	Port	CoS
00-00-00-00-00-01	1	1	High
00-00-00-00-00-02	1	2	Medium
00-00-00-00-00-03	1	3	Normal

**Figure 110: Static MAC Addresses Table**

- Select the MAC address from the table. The **Static MAC Addresses** form appears.



**Figure 111: Static MAC Addresses Form**

- 1. MAC Address Box
- 2. VID Box
- 3. Port Box
- 4. CoS List
- 5. Apply Button
- 6. Delete Button
- 7. Reload Button

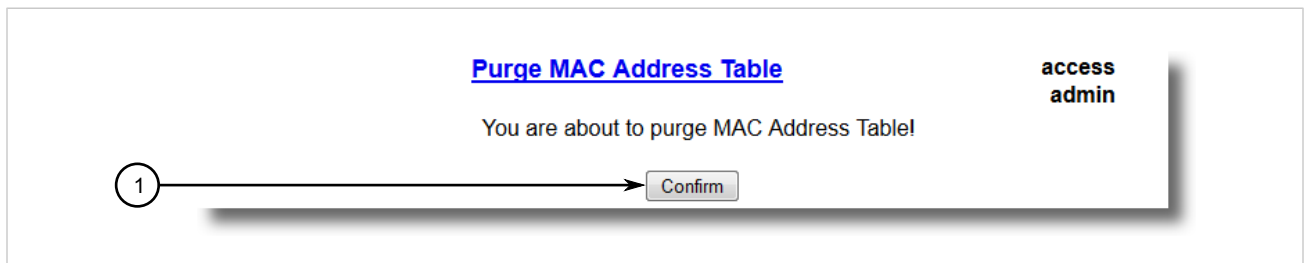
- 3. Click **Delete**.

Section 7.2.5

## Purging All Dynamic MAC Addresses

To purge the dynamic MAC address list of all entries, do the following:

- 1. Navigate to **MAC Address Tables » Purge MAC Address Table**. The **Purge MAC Address Table** form appears.



**Figure 112: Purge MAC Address Table Form**

- 1. Confirm Button

- 2. Click **Confirm**.

## Section 7.3

# Managing Multicast Filtering

Multicast traffic can be filtered using IGMP (Internet Group Management Protocol) snooping or GMRP (GARP Multicast Registration Protocol).

**CONTENTS**

- [Section 7.3.1, "Managing IGMP"](#)
- [Section 7.3.2, "Managing GMRP"](#)

## Section 7.3.1

## Managing IGMP

IGMP is used by IP hosts to report their host group memberships with multicast routers. As hosts join and leave specific multicast groups, streams of traffic are directed to or withheld from that host.

The IGMP protocol operates between multicast routers and IP hosts. When an unmanaged switch is placed between multicast routers and their hosts, the multicast streams will be distributed to all ports. This may introduce significant traffic onto ports that do not require it and receive no benefit from it.

IGMP Snooping, when enabled, will act on IGMP messages sent from the router and the host, restricting traffic streams to the appropriate LAN segments.

**IMPORTANT!**

*RUGGEDCOM ROS restricts IGMP hosts from subscribing to the following special multicast addresses:*

- 224.0.0.0 to 224.0.0.255
- 224.0.1.129

*These addresses are reserved for routing protocols and IEEE 1588. If an IGMP membership report contains one of these addresses, the report is forwarded by the switch without learning about the host.*

**CONTENTS**

- [Section 7.3.1.1, "IGMP Concepts"](#)
- [Section 7.3.1.2, "Viewing a List of Multicast Group Memberships"](#)
- [Section 7.3.1.3, "Viewing Forwarding Information for Multicast Groups"](#)
- [Section 7.3.1.4, "Configuring IGMP"](#)

## Section 7.3.1.1

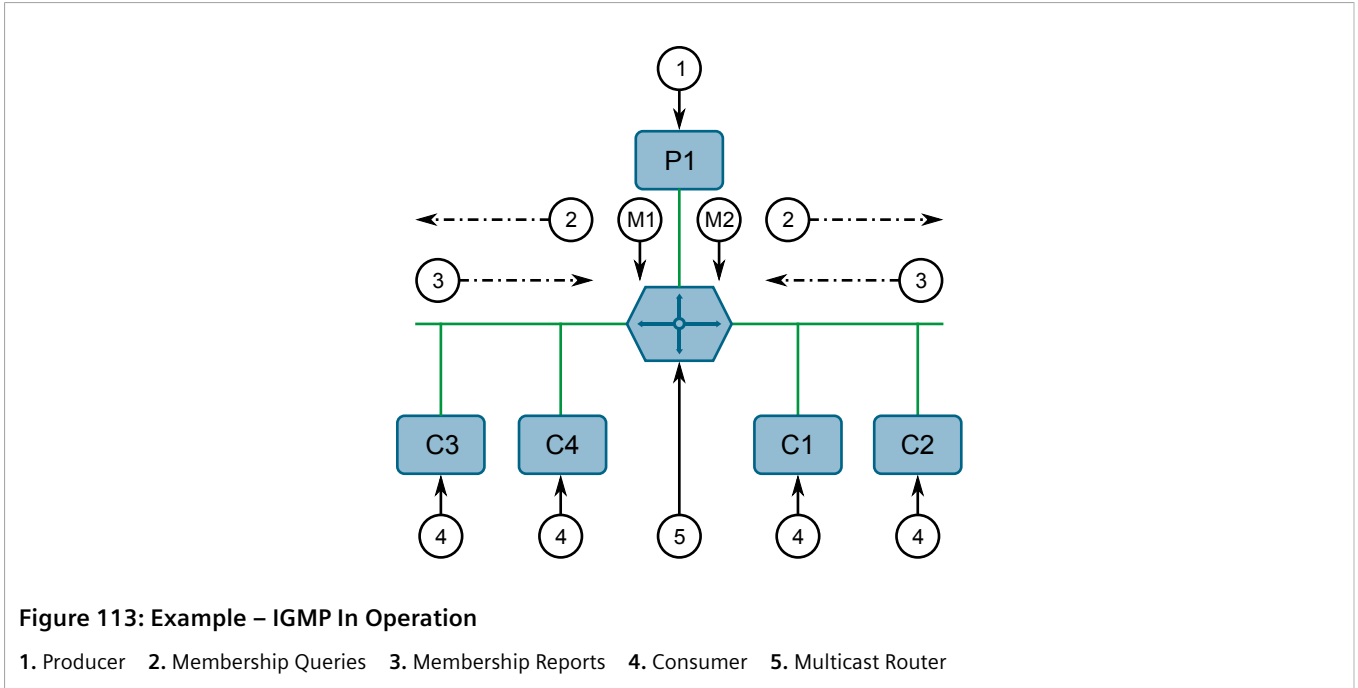
### IGMP Concepts

The following describes some of the concepts important to the implementation of multicast filtering using IGMP:

**>> IGMP In Operation**

The following network diagram provides a simple example of the use of IGMP.





One *producer* IP host (P1) is generating two IP multicast streams, M1 and M2. There are four potential *consumers* of these streams, C1 through C4. The multicast router discovers which host wishes to subscribe to which stream by sending general membership queries to each segment.

In this example, the general membership query sent to the C1-C2 segment is answered by a membership report (or *join*) indicating the desire to subscribe to stream M2. The router will forward the M2 stream to the C1-C2 segment. In a similar fashion, the router discovers that it must forward stream M1 to segment C3-C4.

A *consumer* may join any number of multicast groups, issuing a membership report for each group. When a host issues a membership report, other hosts on the same network segment that also require membership to the same group suppress their own requests, since they would be redundant. In this way, the IGMP protocol guarantees the segment will issue only one membership report for each group.

The router periodically queries each of its segments in order to determine whether at least one consumer still subscribes to a given stream. If it receives no responses within a given time period (usually two query intervals), the router will prune the multicast stream from the given segment.

A more common method of pruning occurs when consumers wishing to unsubscribe issue an IGMP *leave group* message. The router will immediately issue a group-specific membership query to determine whether there are any remaining subscribers of that group on the segment. After the last consumer of a group has unsubscribed, the router will prune the multicast stream from the given segment.

## » Switch IGMP Operation

The IGMP Snooping feature provides a means for switches to snoop (i.e. watch) the operation of routers, respond with joins/leaves on the behalf of consumer ports, and prune multicast streams accordingly. There are two modes of IGMP the switch can be configured to assume: active and passive.

- **Active Mode**

IGMP supports a *routerless* mode of operation.

When such a switch is used without a multicast router, it is able to function as if it is a multicast router sending IGMP general queries.

- **Passive Mode**

When such a switch is used in a network with a multicast router, it can be configured to run Passive IGMP. This mode prevents the switch from sending the queries that can confuse the router causing it to stop issuing IGMP queries.

**NOTE**

*A switch running in passive mode requires the presence of a multicast router or it will be unable to forward multicast streams at all if no multicast routers are present.*

**NOTE**

*At least one IGMP Snooping switch must be in active mode to make IGMP functional.*

## » IGMP Snooping Rules

IGMP Snooping adheres to the following rules:

- When a multicast source starts multicasting, the traffic stream will be immediately blocked on segments from which joins have not been received.
- Unless configured otherwise, the switch will forward all multicast traffic to the ports where multicast routers are attached.
- Packets with a destination IP multicast address in the 224.0.0.X range that are not IGMP are always forwarded to all ports. This behavior is based on the fact that many systems do not send membership reports for IP multicast addresses in this range while still listening to such packets.
- The switch implements IGMPv2 *proxy-reporting* (i.e. membership reports received from downstream are summarized and used by the switch to issue its own reports).
- The switch will only send IGMP membership reports out of those ports where multicast routers are attached, as sending membership reports to hosts could result in unintentionally preventing a host from joining a specific group.
- Multicast routers use IGMP to elect a master router known as the *querier*. The *querier* is the router with the lowest IP address. All other routers become non-queriers, participating only in forwarding multicast traffic. Switches running in active mode participate in the querier election the same as multicast routers.
- When the querier election process is complete, the switch simply relays IGMP queries received from the querier.
- When sending IGMP packets, the switch uses its own IP address, if it has one, for the VLAN on which packets are sent, or an address of 0.0.0.0, if it does not have an assigned IP address.

**NOTE**

*IGMP Snooping switches perform multicast pruning using a multicast frames' destination MAC multicast address, which depends on the group IP multicast address. IP address W.X.Y.Z corresponds to MAC address 01-00-5E-XX-YY-ZZ where XX is the lower 7 bits of X, and YY and ZZ are simply Y and Z coded in hexadecimal.*

*One can note that IP multicast addresses, such as 224.1.1.1 and 225.1.1.1, will both map onto the same MAC address 01-00-5E-01-01-01. This is a problem for which the IETF Network Working Group currently has offered no solution. Users are advised to be aware of and avoid this problem.*

## » IGMP and RSTP

An RSTP change of topology can render the routes selected to carry multicast traffic as incorrect. This results in lost multicast traffic.

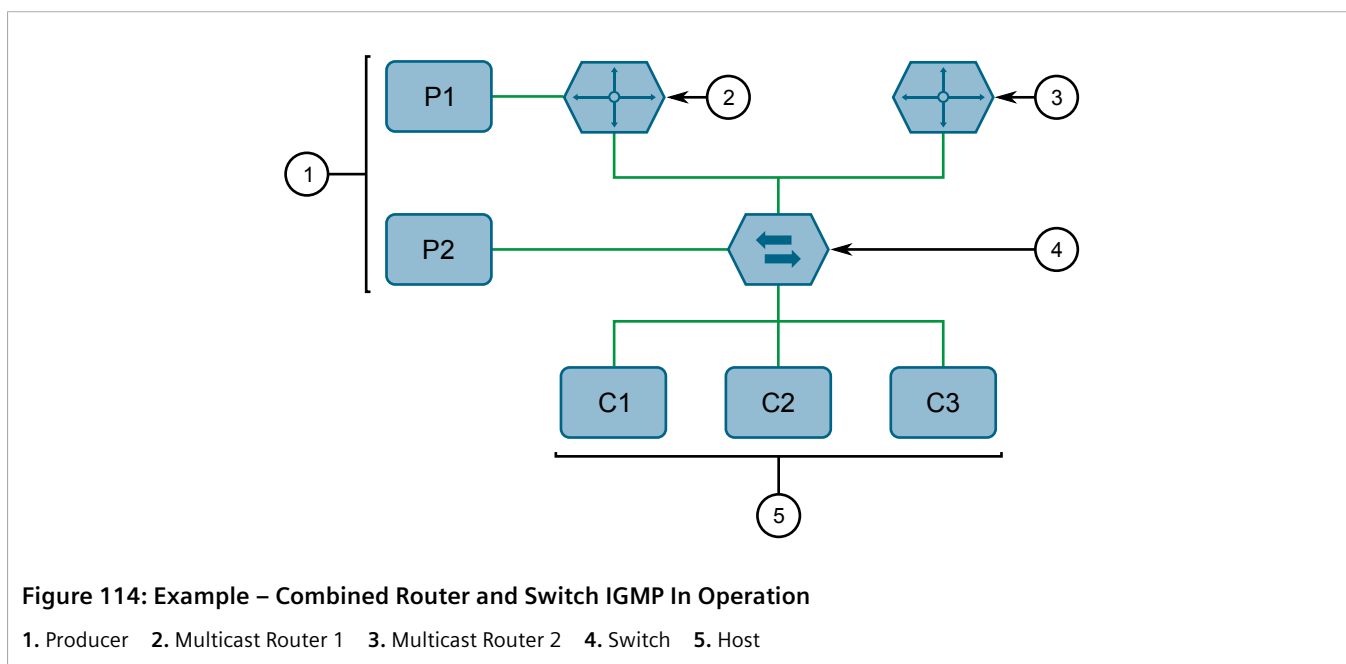
If RSTP detects a change in the network topology, IGMP will take some actions to avoid the loss of multicast connectivity and reduce network convergence time:

- The switch will immediately issue IGMP queries (if in IGMP Active mode) to obtain potential new group membership information.
- The switch can be configured to flood multicast streams temporarily out of all ports that are not configured as RSTP Edge Ports.

## » Combined Router and Switch IGMP Operation

The following example illustrates the challenges faced with multiple routers, VLAN support and switching.

Producer P1 resides on VLAN 2 while P2 resides on VLAN 3. Consumer C1 resides on both VLANs whereas C2 and C3 reside on VLANs 3 and 2, respectively. Router 2 resides on VLAN 2, presumably to forward multicast traffic to a remote network or act as a source of multicast traffic itself.



In this example:

- P1, Router 1, Router 2 and C3 are on VLAN 2
- P2 and C2 are on VLAN 3
- C1 is on both VLAN 2 and 3

Assuming that router 1 is the querier for VLAN 2 and router 2 is simply a non-querier, the switch will periodically receive queries from router 1 and maintain the information concerning which port links to the multicast router. However, the switch port that links to router 2 must be manually configured as a *router port*. Otherwise, the switch will send neither multicast streams nor joins/leaves to router 2.

Note that VLAN 3 does not have an external multicast router. The switch should be configured to operate in its *routerless* mode and issue general membership queries as if it is the router.

### • Processing Joins

If host C1 wants to subscribe to the multicast streams for both P1 and P2, it will generate two membership reports. The membership report from C1 on VLAN 2 will cause the switch to immediately initiate its own membership report to multicast router 1 (and to issue its own membership report as a response to queries).

The membership report from host C1 for VLAN 3 will cause the switch to immediately begin forwarding multicast traffic from producer P2 to host C2.

- **Processing Leaves**

When host C1 decides to leave a multicast group, it will issue a leave request to the switch. The switch will poll the port to determine if host C1 is the last member of the group on that port. If host C1 is the last (or only) member, the group will immediately be pruned from the port.

Should host C1 leave the multicast group without issuing a leave group message and then fail to respond to a general membership query, the switch will stop forwarding traffic after two queries.

When the last port in a multicast group leaves the group (or is aged-out), the switch will issue an IGMP leave report to the router.

## Section 7.3.1.2

## Viewing a List of Multicast Group Memberships

Using IGMP snooping, RUGGEDCOM ROS records group membership information on a per-port basis based on membership reports it observes between the router and host.

To view a list of multicast group memberships, navigate to **Multicast Filtering » View IGMP Group Membership**. The **IGMP Group Membership** table appears.

Port	VID	Group	Ver	Reporter	Age
1	1	224.0.1.0	v3	192.168.0.92	47 s

access admin

Figure 115: IGMP Group Membership Table

This table provides the following information:

Parameter	Description
Port	<b>Synopsis:</b> 1 to maximum port number The port number as seen on the front plate silkscreen of the switch.
VID	<b>Synopsis:</b> 0 to 65535 VLAN Identifier of the VLAN upon which the multicast group operates.
Group	<b>Synopsis:</b> ###.###.###.### where ### ranges from 0 to 255 Multicast Group Address.
Ver	<b>Synopsis:</b> { v3, v2, v1 } Specifies the IGMP version of the learnt multicast group.
Reporter	<b>Synopsis:</b> ###.###.###.### where ### ranges from 0 to 255 Specifies the source IP address that is reporting subscription to the multicast group.
Age	<b>Synopsis:</b> 0 to 7210 s Specifies the current age of the IP multicast group learned on the port in seconds.

If the table is empty, do the following:

- Make sure traffic is being sent to the device.

- Make sure IGMP is properly configured on the device. For more information, refer to [Section 7.3.1.4, "Configuring IGMP"](#).

Section 7.3.1.3

## Viewing Forwarding Information for Multicast Groups

Multicast forwarding information for every source, group and VLAN combination learned by RUGGEDCOM ROS is recorded in the IGMP Multicast Forwarding table.

To view the IGMP Multicast Forwarding table, navigate to **Multicast Filtering » View IGMP Multicast Forwarding**. The **IGMP Multicast Forwarding** table appears.

IGMP Multicast Forwarding				
VID	Group	Source	Joined Ports	Router Ports
1	239.255.255.255	*	2	1

access admin

Figure 116: IGMP Multicast Forwarding Table

This table provides the following information:

Parameter	Description
VID	<b>Synopsis:</b> 0 to 65535 VLAN Identifier of the VLAN upon which the multicast group operates.
Group	<b>Synopsis:</b> ###.###.###.### where ### ranges from 0 to 255 Multicast Group Address.
Source	<b>Synopsis:</b> ###.###.###.### where ### ranges from 0 to 255 or { * } Source Address. * means all possible source addresses.
Joined Ports	<b>Synopsis:</b> Comma-separated list of ports All ports that currently receive multicast traffic for the specified multicast group.
Router Ports	<b>Synopsis:</b> Comma-separated list of ports All ports that have been manually configured or dynamically discovered (by observing router specific traffic) as ports that link to multicast routers.

If the table is empty, do the following:

- Make sure traffic is being sent to the device.
- Make sure IGMP is properly configured on the device. For more information, refer to [Section 7.3.1.4, "Configuring IGMP"](#).

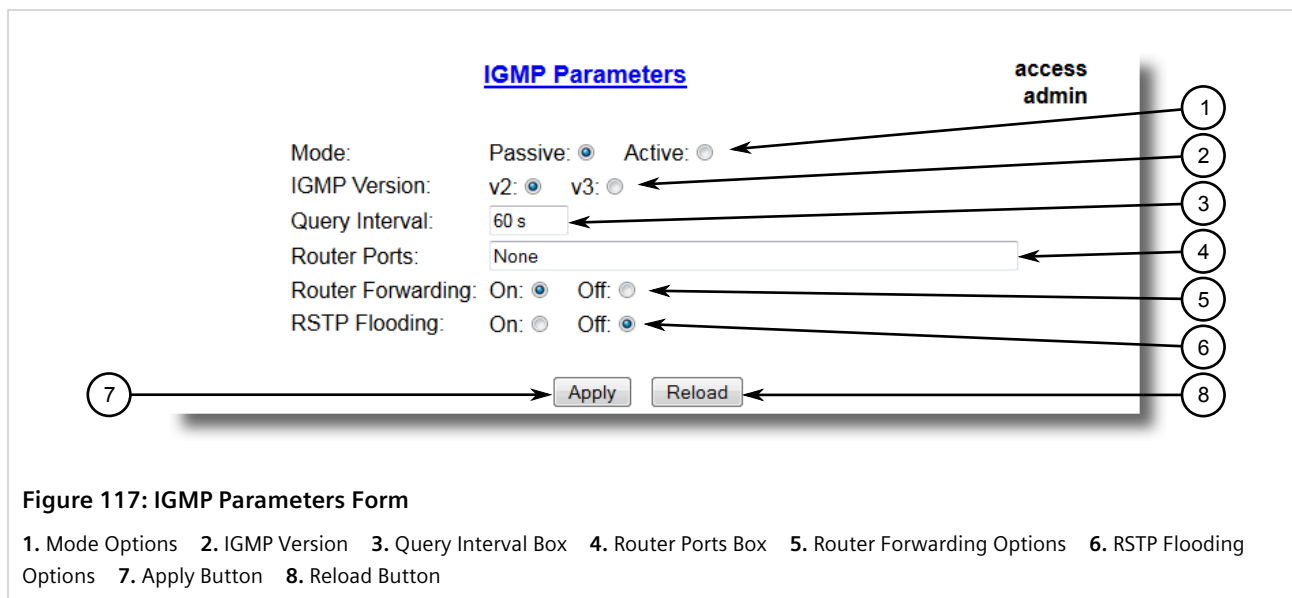
Section 7.3.1.4

## Configuring IGMP

To configure the IGMP, do the following:

1. Make sure one or more static VLANs exist with IGMP enabled. For more information, refer to [Section 7.1.5, "Managing Static VLANs"](#).

2. Navigate to **Multicast Filtering » Configure IGMP Parameters**. The **IGMP Parameters** form appears.



**Figure 117: IGMP Parameters Form**

1. Mode Options 2. IGMP Version 3. Query Interval Box 4. Router Ports Box 5. Router Forwarding Options 6. RSTP Flooding Options 7. Apply Button 8. Reload Button

3. Configure the following parameter(s) as required:

Parameter	Description
Mode	<p><b>Synopsis:</b> { Passive, Active }</p> <p><b>Default:</b> Passive</p> <p>Specifies the IGMP mode. Options include:</p> <ul style="list-style-type: none"> <li>• <b>PASSIVE</b> – the switch passively snoops IGMP traffic and never sends IGMP queries</li> <li>• <b>ACTIVE</b> – the switch generates IGMP queries, if no queries from a better candidate for being the querier are detected for a while.</li> </ul>
IGMP Version	<p><b>Synopsis:</b> { v2, v3 }</p> <p><b>Default:</b> v2</p> <p>Specifies the configured IGMP version on the switch. Options include:</p> <ul style="list-style-type: none"> <li>• <b>v2</b> – Sets the IGMP version to version 2. When selected for a snooping switch, all IGMP reports and queries greater than v2 are forwarded, but not added to the IGMP Multicast Forwarding table.</li> <li>• <b>v3</b> – Sets the IGMP version to version 3. General queries are generated in IGMPv3 format, all versions of IGMP messages are processed by the switch, and traffic is pruned based on multicast group address only.</li> </ul>
Query Interval	<p><b>Synopsis:</b> 10 to 3600</p> <p><b>Default:</b> 60 s</p> <p>The time interval between IGMP queries generated by the switch.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p><b>NOTE</b> This parameter also affects the Group Membership Interval (i.e. the group subscriber aging time), therefore, it takes effect even in <b>PASSIVE</b> mode.</p> </div>
Router Ports	<p><b>Synopsis:</b> Comma-separated list of ports</p> <p><b>Default:</b> None</p> <p>This parameter specifies ports that connect to multicast routers. If you do not configure known router ports, the switch may be able to detect them, however it is advisable to pre-configure them.</p>
Router Forwarding	<p><b>Synopsis:</b> { Off, On }</p> <p><b>Default:</b> On</p>

Parameter	Description
	This parameter specifies whether multicast streams will be always forwarded to multicast routers.
RSTP Flooding	<p><b>Synopsis:</b> { Off, On }</p> <p><b>Default:</b> Off</p> <p>This parameter specifies whether multicast streams will be flooded out of all RSTP non-edge ports upon topology change detection. Such flooding is desirable, if guaranteed multicast stream delivery after topology change is most important.</p>

- Click **Apply**.

### Section 7.3.2

## Managing GMRP

The GMRP is an application of the Generic Attribute Registration Protocol (GARP) that provides a Layer 2 mechanism for managing multicast group memberships in a bridged Layer 2 network. It allows Ethernet switches and end stations to register and unregister membership in multicast groups with other switches on a LAN, and for that information to be disseminated to all switches in the LAN that support Extended Filtering Services.

GMRP is an industry-standard protocol first defined in IEEE 802.1D-1998 and extended in IEEE 802.1Q-2005. GARP was defined in IEEE 802.1D-1998 and updated in 802.1D-2004.



#### NOTE

*GMRP provides similar functionality at Layer 2 to what IGMP provides at Layer 3.*

#### CONTENTS

- [Section 7.3.2.1, "GMRP Concepts"](#)
- [Section 7.3.2.2, "Viewing a Summary of Multicast Groups"](#)
- [Section 7.3.2.3, "Configuring GMRP Globally"](#)
- [Section 7.3.2.4, "Configuring GMRP for Specific Ethernet Ports"](#)
- [Section 7.3.2.5, "Viewing a List of Static Multicast Groups"](#)
- [Section 7.3.2.6, "Adding a Static Multicast Group"](#)
- [Section 7.3.2.7, "Deleting a Static Multicast Group"](#)

### Section 7.3.2.1

## GMRP Concepts

The following describes some of the concepts important to the implementation of multicast filtering using GMRP:

### » Joining a Multicast Group

To join a multicast group, an end station transmits a GMRP *join* message. The switch that receives the *join* message adds the port through which the message was received to the multicast group specified in the message. It then propagates the *join* message to all other hosts in the VLAN, one of which is expected to be the multicast source.

When a switch transmits GMRP updates (from GMRP-enabled ports), all of the multicast groups known to the switch, whether configured manually or learned dynamically through GMRP, are advertised to the rest of network. As long as one host on the Layer 2 network has registered for a given multicast group, traffic from the corresponding multicast source will be carried on the network. Traffic multicast by the source is only forwarded by each switch in the network to those ports from which it has received join messages for the multicast group.

### » Leaving a Multicast Group

Periodically, the switch sends GMRP queries in the form of a *leave all* message. If a host (either a switch or an end station) wishes to remain in a multicast group, it reasserts its group membership by responding with an appropriate *join* request. Otherwise, it can either respond with a *leave* message or simply not respond at all. If the switch receives a *leave* message or receives no response from the host for a timeout period, the switch removes the host from the multicast group.

### » Notes About GMRP

Since GMRP is an application of GARP, transactions take place using the GARP protocol. GMRP defines the following two Attribute Types:

- The Group Attribute Type, used to identify the values of group MAC addresses
- The Service Requirement Attribute Type, used to identify service requirements for the group

Service Requirement Attributes are used to change the receiving port's multicast filtering behavior to one of the following:

- Forward All Multicast group traffic in the VLAN, or
- Forward All Unknown Traffic (Multicast Groups) for which there are no members registered in the device in a VLAN

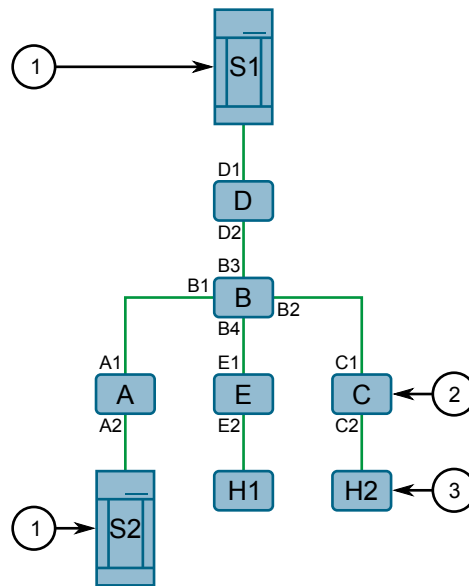
If GMRP is disabled, GMRP packets received will be forwarded like any other traffic. Otherwise, GMRP packets will be processed and not forwarded.

### » Establishing Membership with GMRP

The following example illustrates how a network of hosts and switches can dynamically join two multicast groups using GMRP.

In this scenario, there are two multicast sources, S1 and S2, multicasting to Multicast Groups 1 and 2, respectively. A network of five switches, including one core switch (B), connects the sources to two hosts, H1 and H2, which receive the multicast streams from S1 and S2, respectively.





**Figure 118: Example – Establishing Membership with GMRP**

1. Multicast Source 2. Switch 3. Multicast Host

The hosts and switches establish membership with the Multicast Group 1 and 2 as follows:

1. Host H1 is GMRP unaware, but needs to see traffic for Multicast Group 1. Therefore, Port E2 on Switch E is statically configured to forward traffic for Multicast Group 1.
2. Switch E advertises membership in Multicast Group 1 to the network through Port E1, making Port B4 on Switch B a member of Multicast Group 1.
3. Switch B propagates the *join* message, causing Ports A1, C1 and D1 to become members of Multicast Group 1.
4. Host H2 is GMRP-aware and sends a *join* request for Multicast Group 2 to Port C2, which thereby becomes a member of Multicast Group 2.
5. Switch C propagates the *join* message, causing Ports A1, B2, D1 and E1 to become members of Multicast Group 2.

Once GMRP-based registration has propagated through the network, multicast traffic from S1 and S2 can reach its destination as follows:

- Source S1 transmits multicast traffic to Port D2 which is forwarded via Port D1, which has previously become a member of Multicast Group 1.
- Switch B forwards the Group 1 multicast via Port B4 towards Switch E.
- Switch E forwards the Group 1 multicast via Port E2, which has been statically configured for membership in Multicast Group 1.
- Host H1, connected to Port E2, thus receives the Group 1 multicast.
- Source S2 transmits multicast traffic to Port A2, which is then forwarded via port A1, which has previously become a member of Multicast Group 2.
- Switch B forwards the Group 2 multicast via Port B2 towards Switch C.
- Switch C forwards the Group 2 multicast via Port C2, which has previously become a member of Group 2.
- Ultimately, Host H2, connected to Port C2, receives the Group 2 multicast.

## Section 7.3.2.2

## Viewing a Summary of Multicast Groups

To view a summary of all multicast groups, navigate to **Multicast Filtering » View Multicast Group Summary**. The **Multicast Group Summary** table appears.

<b>Multicast Group Summary</b>			
VID	MAC Address	Static Ports	GMRP Dynamic Ports
<a href="#">1</a>	01-00-5E-7F-FF-FA	None	None
<a href="#">1</a>	33-33-00-01-00-02	None	None
<a href="#">4</a>	01-00-5E-00-04-00	1	None

access  
admin

**Figure 119: Multicast Group Summary Table**

This table provides the following information:

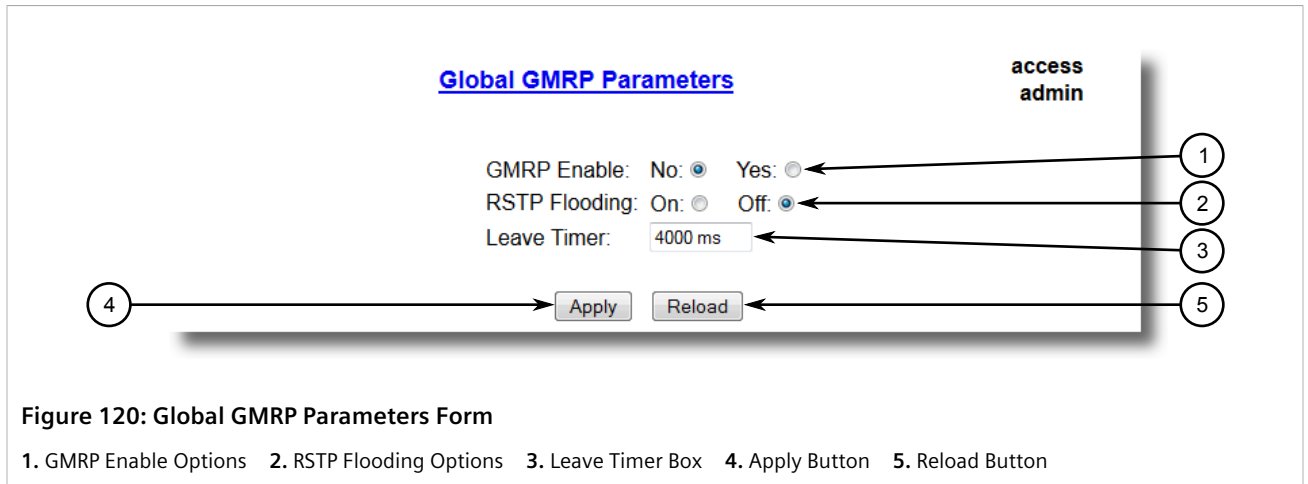
Parameter	Description
VID	<b>Synopsis:</b> 0 to 65535 VLAN Identifier of the VLAN upon which the multicast group operates.
MAC Address	<b>Synopsis:</b> ##-##-##-##-##-## where ## ranges 0 to FF Multicast group MAC address.
Static Ports	<b>Synopsis:</b> Any combination of numbers valid for this parameter Ports that joined this group statically through static configuration in Static MAC Table and to which the multicast group traffic is forwarded.
GMRP Dynamic Ports	<b>Synopsis:</b> Any combination of numbers valid for this parameter Ports that joined this group dynamically through GMRP Application and to which the multicast group traffic is forwarded.

## Section 7.3.2.3

## Configuring GMRP Globally

To configure global settings for GMRP, do the following:

1. Navigate to **Multicast Filtering » Configure Global GMRP Parameters**. The **Global GMRP Parameters** form appears.



**Figure 120: Global GMRP Parameters Form**

1. GMRP Enable Options 2. RSTP Flooding Options 3. Leave Timer Box 4. Apply Button 5. Reload Button

2. Configure the following parameter(s) as required:

Parameter	Description
GMRP Enable	<p><b>Synopsis:</b> { No, Yes }</p> <p><b>Default:</b> No</p> <p>Globally enable or disable GMRP.</p> <p>When GMRP is globally disabled, GMRP configurations on individual ports are ignored. When GMRP is globally enabled, each port can be individually configured.</p>
RSTP Flooding	<p><b>Synopsis:</b> { On, Off }</p> <p><b>Default:</b> Off</p> <p>This parameter specifies whether multicast streams will be flooded out of all RSTP non-edge ports upon topology change detection. Such flooding is desirable, if guaranteed multicast stream delivery after topology change is most important.</p>
Leave Timer	<p><b>Synopsis:</b> 600 to 300000 ms</p> <p><b>Default:</b> 4000 ms</p> <p>Time (milliseconds) to wait after issuing Leave or LeaveAll before removing registered multicast groups. If Join messages for specific addresses are received before this timer expires, the addresses will be kept registered.</p>

3. Click **Apply**.

Section 7.3.2.4

## Configuring GMRP for Specific Ethernet Ports

To configure GMRP for a specific Ethernet port, do the following:

1. Make sure the global settings for GMRP have been configured. For more information, refer to [Section 7.3.2.3, "Configuring GMRP Globally"](#).
2. Navigate to **Multicast Filtering » Configure Port GMRP Parameters**. The **Port GMRP Parameters** table appears.

**access  
admin**

Port(s)	GMRP
<a href="#">1</a>	Disabled
<a href="#">2</a>	Disabled
<a href="#">3</a>	Disabled
<a href="#">4</a>	Disabled
<a href="#">5</a>	Disabled
<a href="#">6</a>	Disabled
<a href="#">7</a>	Disabled
<a href="#">8</a>	Disabled
<a href="#">9</a>	Disabled
<a href="#">10</a>	Disabled

**Figure 121: Port GMRP Parameters Table**

- Select an Ethernet port. The **Port GMRP Parameters** form appears.

**access  
admin**

Port(s):  ← 1

GMRP:  ← 2

← 3     ← 4

**Figure 122: Port GMRP Parameters Form**

- Port(s) Box
- GMRP List
- Apply Button
- Reload Button

- Configure the following parameter(s) as required:

Parameter	Description
Port(s)	<p><b>Synopsis:</b> Any combination of numbers valid for this parameter</p> <p>The port number as seen on the front plate silkscreen of the switch (or a list of ports, if aggregated in a port trunk).</p>
GMRP	<p><b>Synopsis:</b> { Disabled, Adv Only, Adv&amp;Learn }</p> <p><b>Default:</b> Default: Disabled</p> <p>Configures GMRP (GARP Multicast Registration Protocol) operation on the port. There are several GMRP operation modes:</p> <ul style="list-style-type: none"> <li>DISABLED - the port is not capable of any GMRP processing.</li> <li>ADVERTISE ONLY - the port will declare all MCAST addresses existing in the switch (configured or learned) but will not learn any MCAST addresses.</li> <li>ADVERTISE &amp; LEARN - the port will declare all MCAST Addresses existing in the switch (configured or learned) and can dynamically learn MCAST addresses.</li> </ul>

- Click **Apply**.

Section 7.3.2.5

## Viewing a List of Static Multicast Groups

To view a list of static multicast groups, navigate to *Multicast Filtering » Configure Static Multicast Groups*. The **Static Multicast Groups** table appears.

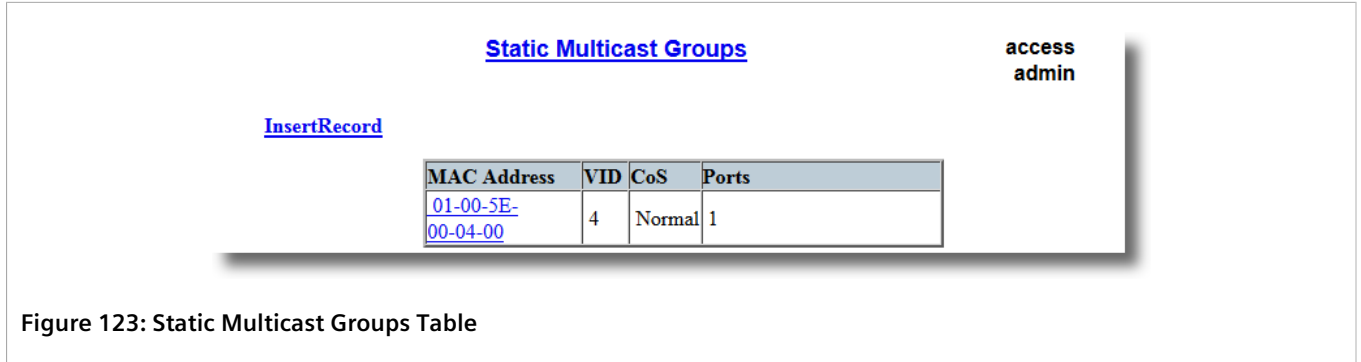


Figure 123: Static Multicast Groups Table

If a static multicast group is not listed, add the group. For more information, refer to [Section 7.3.2.6, "Adding a Static Multicast Group"](#).

Section 7.3.2.6

## Adding a Static Multicast Group

To add a static multicast group from another device, do the following:

1. Navigate to *Multicast Filtering » Configure Static Multicast Groups*. The **Static Multicast Groups** table appears.

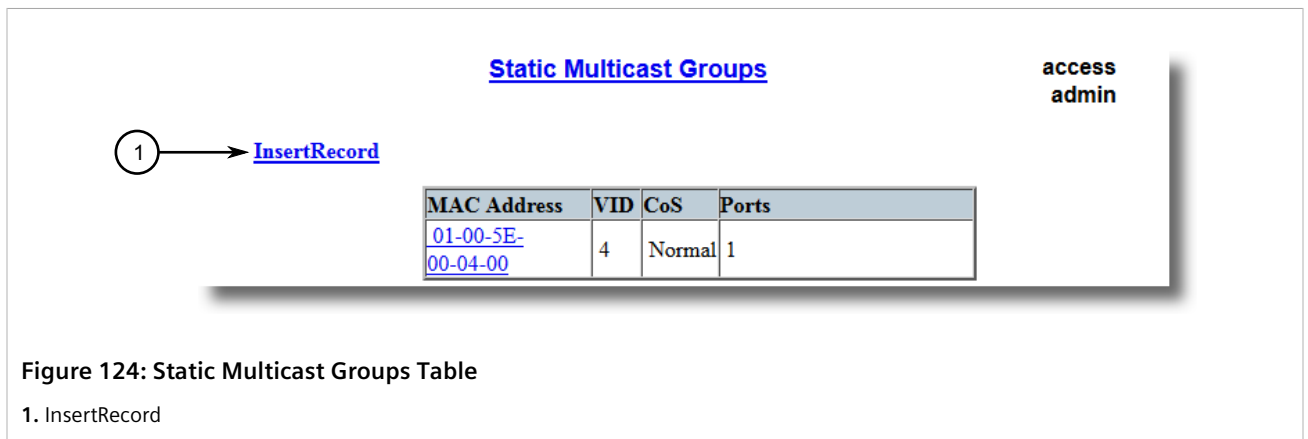
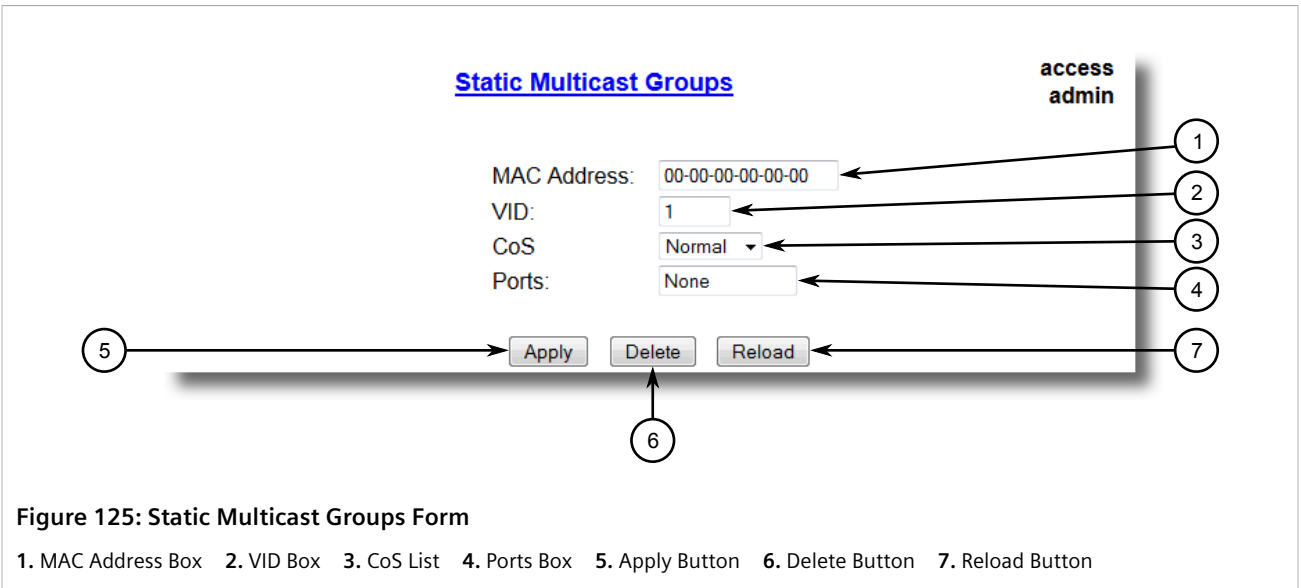


Figure 124: Static Multicast Groups Table

1. InsertRecord

2. Click **InsertRecord**. The **Static Multicast Groups** form appears.



3. Configure the following parameter(s) as required:

Parameter	Description
MAC Address	<b>Synopsis:</b> ##-##-##-##-##-## where ## ranges 0 to FF <b>Default:</b> 00-00-00-00-00-00 Multicast group MAC address.
VID	<b>Synopsis:</b> 1 to 4094 <b>Default:</b> 1 VLAN Identifier of the VLAN upon which the multicast group operates.
CoS	<b>Synopsis:</b> { N/A, Normal, Medium, High, Crit } <b>Default:</b> N/A Prioritizes traffic for the specified MAC address. To not prioritize traffic based on the address, select N/A.
Ports	<b>Synopsis:</b> Any combination of numbers valid for this parameter <b>Default:</b> None Ports to which the multicast group traffic is forwarded.

4. Click **Apply**.

Section 7.3.2.7

## Deleting a Static Multicast Group

To delete a static multicast group, do the following:

1. Navigate to **Multicast Filtering » Configure Static Multicast Groups**. The **Static Multicast Groups** table appears.

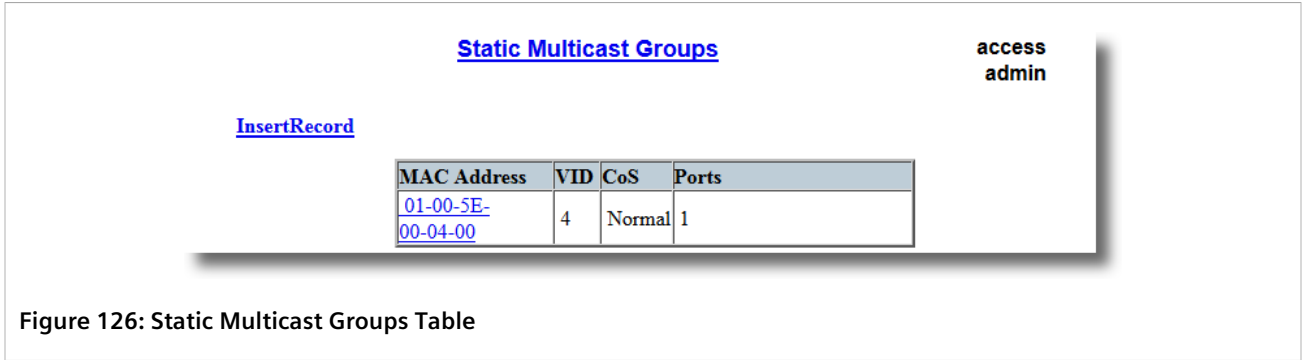


Figure 126: Static Multicast Groups Table

2. Select the group from the table. The **Static Multicast Groups** form appears.

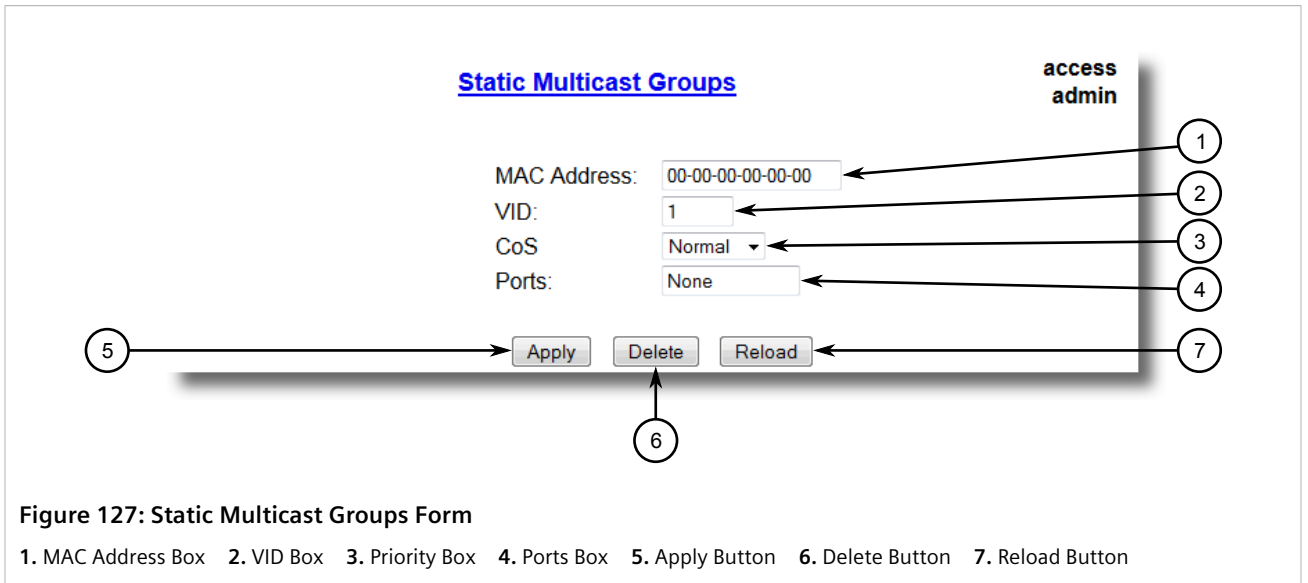


Figure 127: Static Multicast Groups Form

1. MAC Address Box
2. VID Box
3. Priority Box
4. Ports Box
5. Apply Button
6. Delete Button
7. Reload Button

3. Click **Delete**.





# 8 Traffic Control and Classification

Use the traffic control and classification subsystems to control the flow of data packets to connected network interfaces.

## CONTENTS

- [Section 8.1, “Managing Classes of Service”](#)

### Section 8.1

## Managing Classes of Service

Classes of Service (CoS) provides the ability to expedite the transmission of certain frames and port traffic over others. The CoS of a frame can be set to Normal, Medium, High, or Critical. By default, other than the control frames, RUGGEDCOM ROS enforces Normal CoS for all incoming traffic received without a priority tag.



### IMPORTANT!

*Use the highest supported CoS with caution, as it is always used by the switch for handling network management traffic, such as RSTP BPDUs.*

*If this CoS is used for regular network traffic, upon traffic bursts, it may result in the loss of some network management frames, which in turn may result in the loss of connectivity over the network.*

The process of controlling traffic based on CoS occurs over two phases:

#### 1. Inspection Phase

In the inspection phase, the CoS priority of a received frame is determined from either:

- A specific CoS based upon the source and destination MAC address (as set in the Static MAC Address Table)
- The priority field in the IEEE 802.1Q tags
- The Differentiated Services Code Point (DSCP) component of the Type Of Service (TOS) field in the IP header, if the frame is IP
- The default CoS for the port

Each frame’s CoS will be determined once the first examined parameter is found in the frame.



### NOTE

*For information on how to configure the **Inspect TOS** parameter, refer to [Section 8.1.2, “Configuring Classes of Service for Specific Ethernet Ports”](#).*

Received frames are first examined to determine if their destination or source MAC address is found in the Static MAC Address Table. If they are, the CoS configured for the static MAC address is used. If neither destination or source MAC address is in the Static MAC Address Table, the frame is then examined for IEEE 802.1Q tags and the priority field is mapped to a CoS. If a tag is not present, the frame is examined to determine if it is an IP frame. If the frame is an IP frame and **Inspect TOS** is enabled in RUGGEDCOM ROS, the

CoS is determined from the DSCP field. If the frame is not an IP frame or **Inspect TOS** is disabled, the default CoS for the port is used.

After inspection, the frame is forwarded to the egress port for transmission.

## 2. Forwarding Phase

Once the CoS of the frame is determined, the frame is forwarded to the egress port, where it is collected into one of the priority queues according to the assigned CoS.

CoS weighting selects the degree of preferential treatment that is attached to different priority queues. The ratio of the number of higher CoS to lower CoS frames transmitted can be configured. If desired, lower CoS frames can be transmitted only after all higher CoS frames have been serviced.

### CONTENTS

- [Section 8.1.1, "Configuring Classes of Service Globally"](#)
- [Section 8.1.2, "Configuring Classes of Service for Specific Ethernet Ports"](#)
- [Section 8.1.3, "Configuring Priority to CoS Mapping"](#)
- [Section 8.1.4, "Configuring DSCP to CoS Mapping"](#)

#### Section 8.1.1

## Configuring Classes of Service Globally

To configure global settings for Classes of Service (CoS), do the following:

1. Navigate to **Classes of Service » Configure Global CoS Parameters**. The **Global CoS Parameters** form appears.



2. Configure the following parameter(s) as required:

Parameter	Description
CoS Weighting	<p><b>Synopsis:</b> { 8:4:2:1, Strict }</p> <p><b>Default:</b> 8:4:2:1</p> <p>During traffic bursts, frames queued in the switch pending transmission on a port may have different CoS priorities. This parameter specifies weighting algorithm for transmitting different priority CoS frames.</p> <p>Examples:</p> <ul style="list-style-type: none"> <li>• 8:4:2:1 - 8 Critical, 4 High, 2 Medium and 1 Normal priority CoS frame</li> <li>• Strict - lower priority CoS frames will be only transmitted after all higher priority CoS frames have been transmitted</li> </ul>

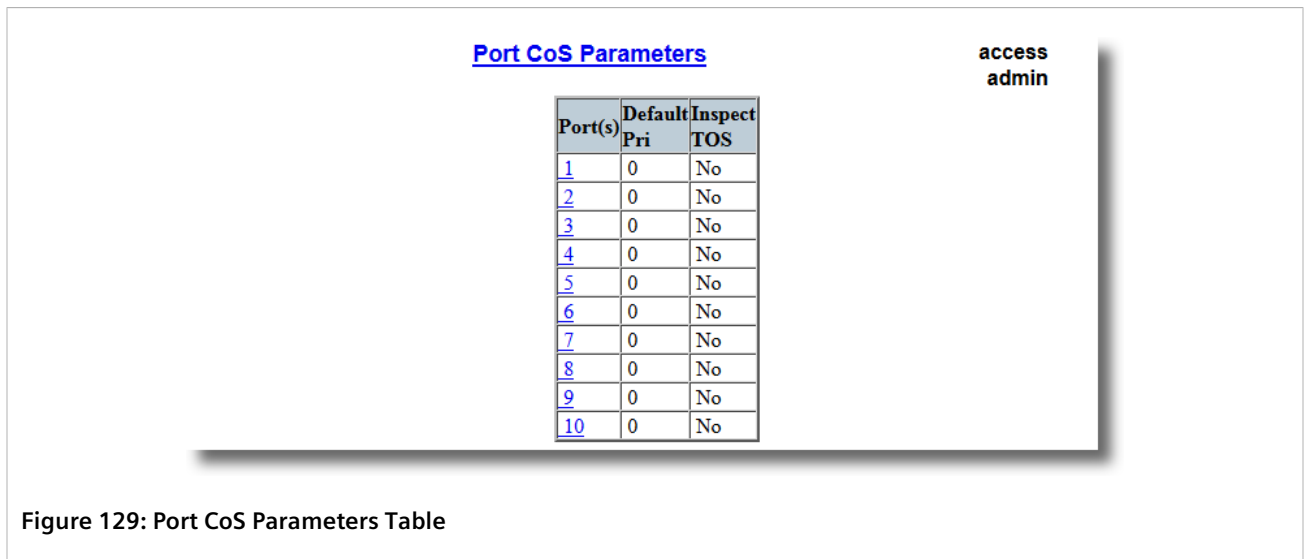
3. Click **Apply**.
4. If necessary, configure CoS mapping based on either the IEEE 802.1p priority or Differentiated Services (DS) field set in the IP header for each packet. For more information, refer to [Section 8.1.3, "Configuring Priority to CoS Mapping"](#) or [Section 8.1.4, "Configuring DSCP to CoS Mapping"](#).

Section 8.1.2

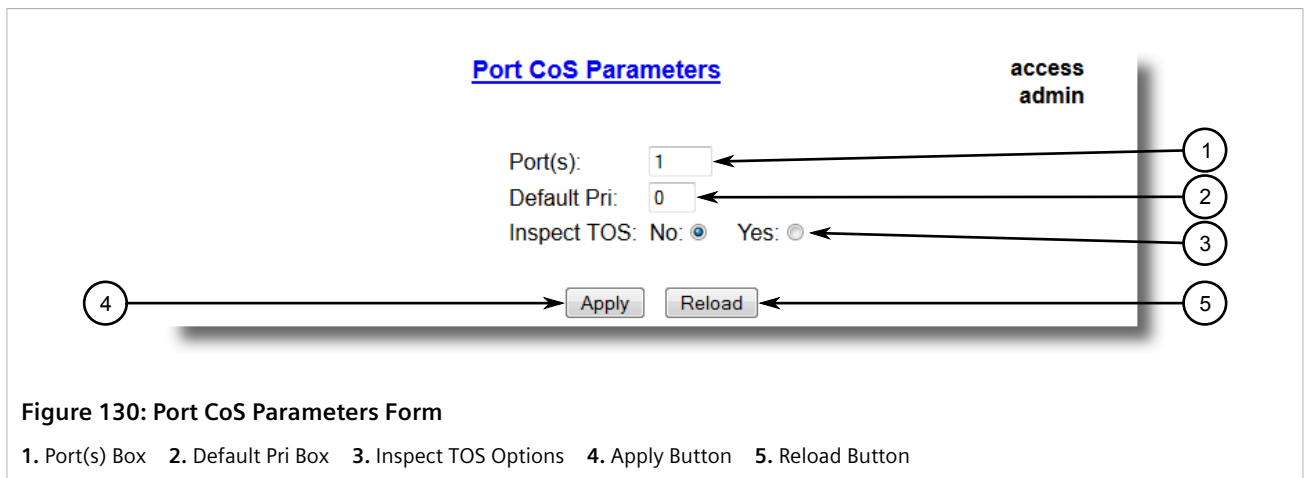
## Configuring Classes of Service for Specific Ethernet Ports

To configure Classes of Service (CoS) for one or more Ethernet ports, do the following:

1. Navigate to **Classes of Service » Configure Port CoS Parameters**. The **Port CoS Parameters** table appears.



2. Select an Ethernet port. The **Port CoS Parameters** form appears.



3. Configure the following parameter(s) as required:

Parameter	Description
Port(s)	<b>Synopsis:</b> Any combination of numbers valid for this parameter

Parameter	Description
	The port number as seen on the front plate silkscreen of the switch (or a list of ports, if aggregated in a port trunk).
Default Pri	<b>Synopsis:</b> 0 to 7 <b>Default:</b> 0  This parameter allows to prioritize frames received on this port that are not prioritized based on the frames contents (e.g. priority field in the VLAN tag, DiffServ field in the IP header, prioritized MAC address).
Inspect TOS	<b>Synopsis:</b> { No, Yes } <b>Default:</b> No  This parameters enables or disables parsing of the Type-Of-Service (TOS) field in the IP header of the received frames to determine what Class of Service they should be assigned. When TOS parsing is enabled the switch will use the Differentiated Services bits in the TOS field.

- Click **Apply**.

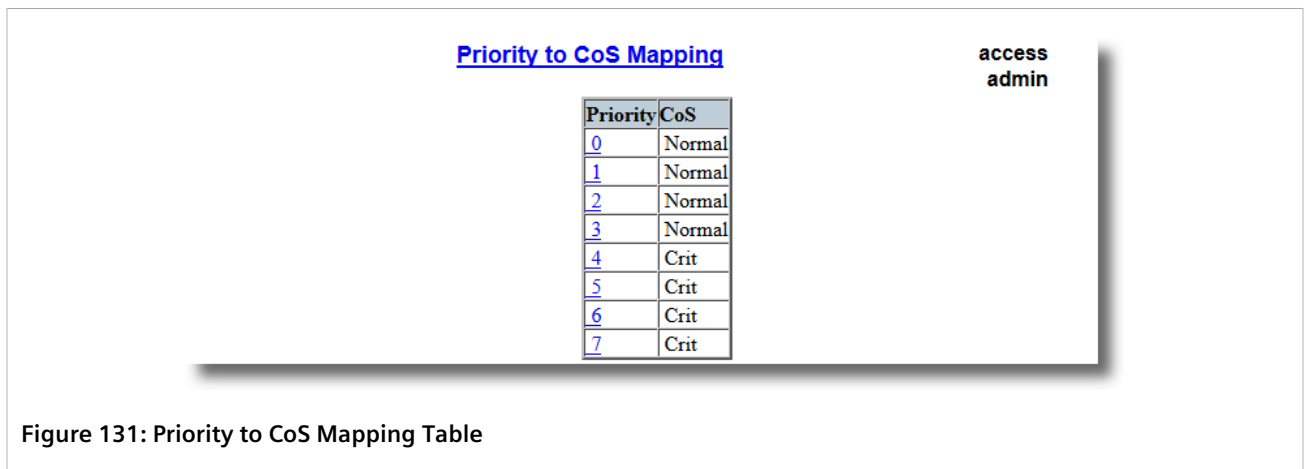
Section 8.1.3

## Configuring Priority to CoS Mapping

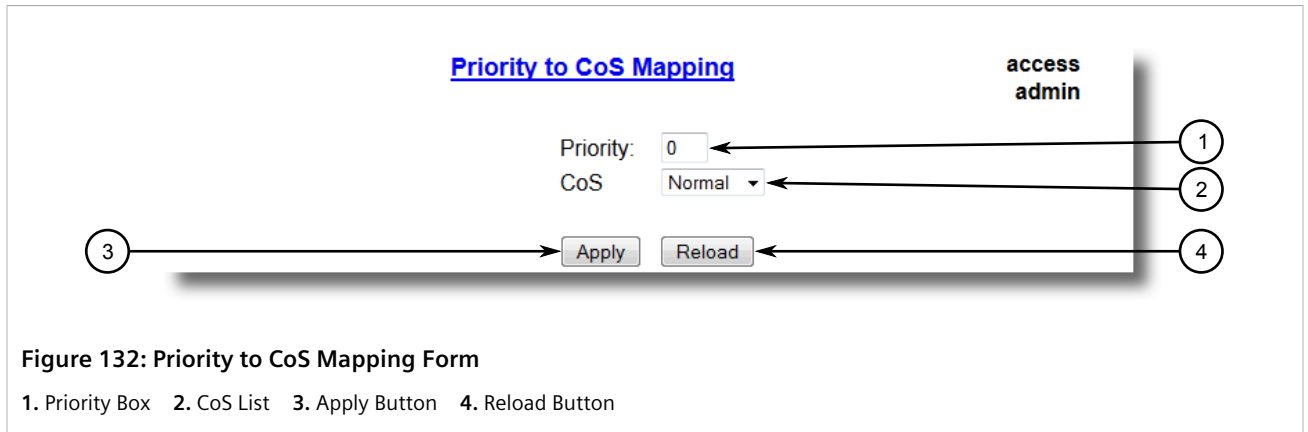
Frames received untagged can be automatically assigned a CoS based on their priority level.

To map a priority level to a CoS, do the following:

- Navigate to **Classes of Service » Configure Priority to CoS Mapping**. The **Priority to CoS Mapping** table appears.



- Select a priority level. The **Priority to CoS Mapping** form appears.



- Configure the following parameter(s) as required:

Parameter	Description
Priority	<p><b>Synopsis:</b> 0 to 7</p> <p><b>Default:</b> 0</p> <p>Value of the IEEE 802.1p priority.</p>
CoS	<p><b>Synopsis:</b> { Normal, Medium, High, Crit }</p> <p><b>Default:</b> Normal</p> <p>CoS assigned to received tagged frames with the specified IEEE 802.1p priority value.</p>

- Click **Apply**.

Section 8.1.4

## Configuring DSCP to CoS Mapping

Mapping CoS to the Differentiated Services (DS) field set in the IP header for each packet is done by defining Differentiated Services Code Points (DSCPs) in the CoS configuration.

To map a DSCP to a Class of Service, do the following:

- Navigate to **Classes of Service » Configure DSCP to CoS Mapping**. The **DSCP to CoS Mapping** table appears.

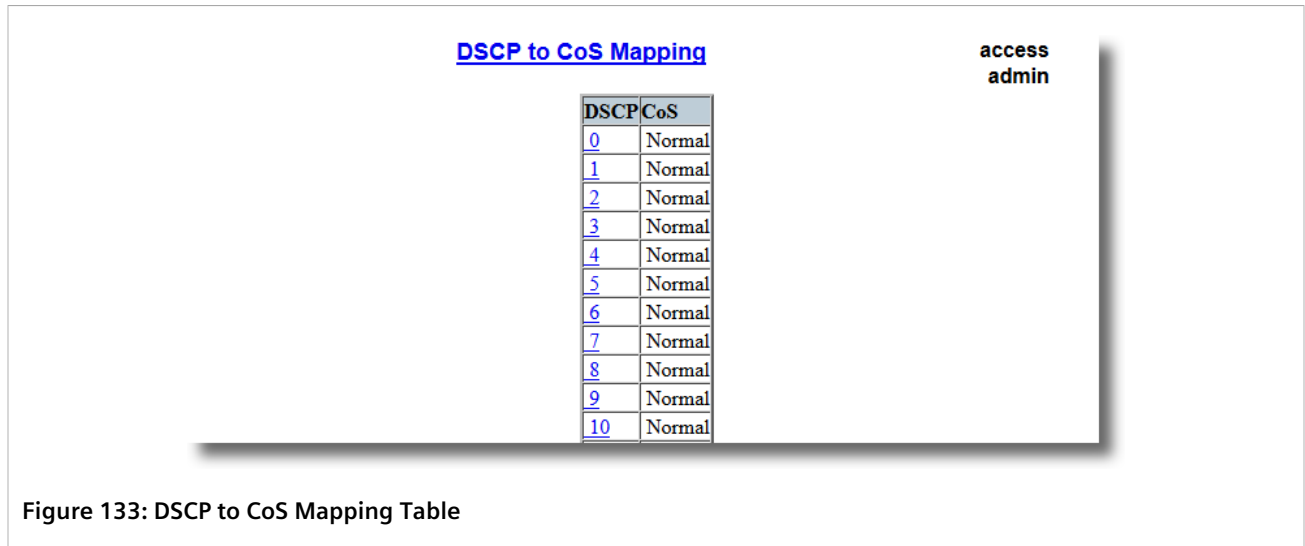


Figure 133: DSCP to CoS Mapping Table

- Select a DSCP level. The **DSCP to CoS Mapping** form appears.

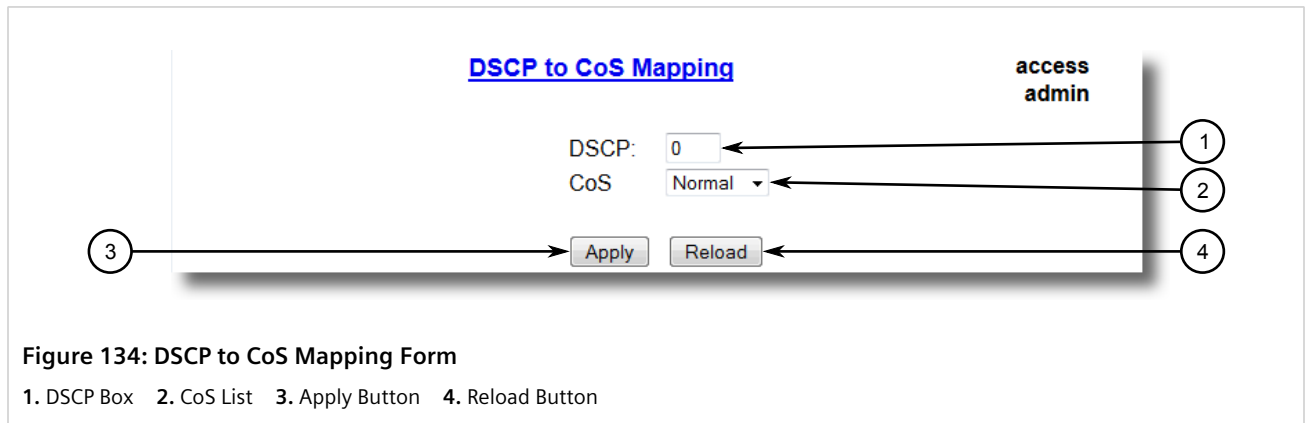


Figure 134: DSCP to CoS Mapping Form

- DSCP Box
- CoS List
- Apply Button
- Reload Button

- Configure the following parameter(s) as required:

Parameter	Description
DSCP	<p><b>Synopsis:</b> 0 to 63  <b>Default:</b> 0</p> <p>Differentiated Services Code Point (DSCP) - a value of the 6 bit DiffServ field in the Type-Of-Service (TOS) field of the IP header.</p>
CoS	<p><b>Synopsis:</b> { Normal, Medium, High, Crit }</p> <p><b>Default:</b> Normal</p> <p>Class of Service assigned to received frames with the specified DSCP.</p>

- Click **Apply**.
- Configure the CoS parameters on select switched Ethernet ports as needed. For more information, refer to [Section 8.1.2, "Configuring Classes of Service for Specific Ethernet Ports"](#).

# 9 Time Services

This chapter describes the time-keeping and time synchronization features in RUGGEDCOM ROS.

## CONTENTS

- [Section 9.1, "Configuring the Time and Date"](#)
- [Section 9.2, "Managing NTP"](#)

### Section 9.1

## Configuring the Time and Date

To set the time, date and other time-keeping related parameters, do the following:

1. Navigate to **Administration » System Time Manager » Configure Time and Date**. The **Time and Date** form appears.

**Figure 135: Time and Date Form**

1. Time 2. Date 3. Time Zone 4. DST Offset 5. DST Rule 6. Apply Button 7. Reload Button

2. Configure the following parameter(s) as required:

Parameter	Description
Time	<b>Synopsis:</b> HH:MM:SS This parameter allows for both the viewing and setting of the local time.
Date	<b>Synopsis:</b> MMM DD, YYYY This parameter allows for both the viewing and setting of the local date.
Time Zone	<b>Synopsis:</b> { UTC-12:00 (Eniwetok, Kwajalein), UTC-11:00 (Midway Island, Samoa), UTC-10:00 (Hawaii), UTC-9:00 (Alaska), UTC-8:00 (Los Angeles, Vancouver), UTC-7:00

Parameter	Description
	(Calgary, Denver), UTC-6:00 (Chicago, Mexico City), UTC-5:00 (New York, Toronto), UTC-4:30 (Caracas), UTC-4:00 (Santiago), UTC-3:30 (Newfoundland), UTC-3:00 (Brasilia, Buenos Aires), UTC-2:00 (Mid Atlantic), UTC-1:00 (Azores), UTC-0:00 (Lisbon, London), UTC+1:00 (Berlin, Paris, Rome), UTC+2:00 (Athens, Cairo, Helsinki), ... } <b>Default:</b> UTC-5:00 (New York, Toronto) This setting allows for the conversion of UTC (Universal Coordinated Time) to local time.
DST Offset	<b>Synopsis:</b> HH:MM:SS <b>Default:</b> 00:00:00 This parameter specifies the amount of time to be shifted forward/backward when DST begins and ends. For example for most part of USA and Canada, DST time shift is 1 hour (01:00:00) forward when DST begins and 1 hour backward when DST ends.
DST Rule	<b>Synopsis:</b> mm.n.d/HH:MM:SS mm.n.d/HH:MM:SS This parameter specifies a rule for time and date when the transition between Standard and Daylight Saving Time occurs. <ul style="list-style-type: none"> <li>• mm - Month of the year (01 - January, 12 - December)</li> <li>• n - nth d-day in the month (1 - 1st d-day, 5 - 5th/last d-day)</li> <li>• d - day of the week (0 - Sunday, 6 - Saturday)</li> <li>• HH - hour of the day (0 - 24)</li> <li>• MM - minute of the hour (0 - 59)</li> <li>• SS - second of the minute (0 - 59)</li> </ul> Example: The following rule applies in most part of USA and Canada: <pre>03.2.0/02:00:00 11.1.0/02:00:00</pre> DST begins on March's 2nd Sunday at 2:00am. DST ends on November's 1st Sunday at 2:00am.

## Section 9.2

## Managing NTP

RUGGEDCOM ROS may be configured to refer periodically to a specified NTP server to correct any accumulated drift in the on-board clock. RUGGEDCOM ROS will also serve time via the Simple Network Time Protocol (SNTP) to hosts that request it.

Two NTP servers (primary and backup) may be configured for the device. The primary server is contacted first for each attempt to update the system time. If the primary server fails to respond, the backup server is contacted. If either the primary or backup server fails to respond, an alarm is raised.

**CONTENTS**

- [Section 9.2.1, "Enabling/Disabling NTP Service"](#)
- [Section 9.2.2, "Configuring NTP Servers"](#)

## Section 9.2.1

### Enabling/Disabling NTP Service

To enable or disable NTP Service, do the following:

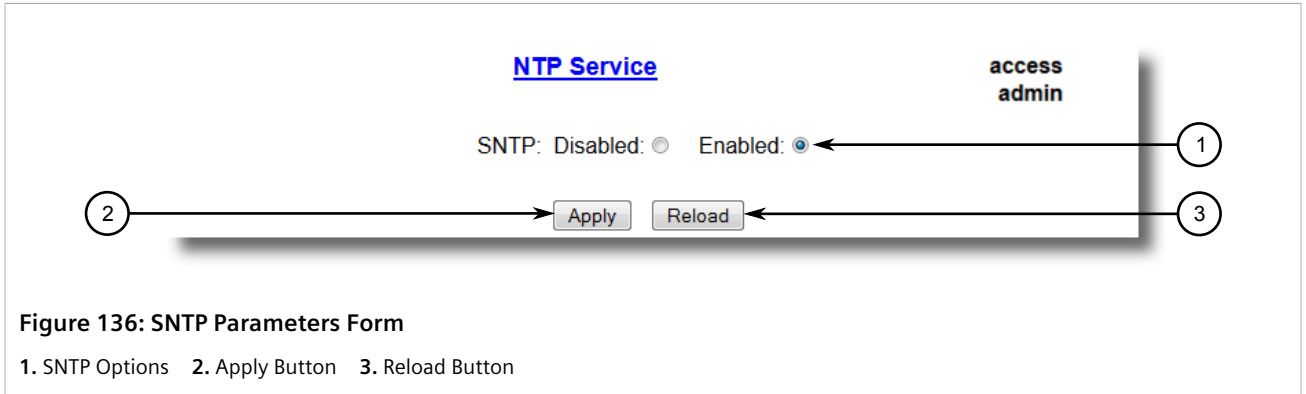




**NOTE**

*If the device is running as an NTP server, NTP service must be enabled.*

1. Navigate to **Administration » System Time Manager » Configure NTP » Configure NTP Service**. The **SNTP Parameters** form appears.



**Figure 136: SNTP Parameters Form**

1. SNTP Options 2. Apply Button 3. Reload Button

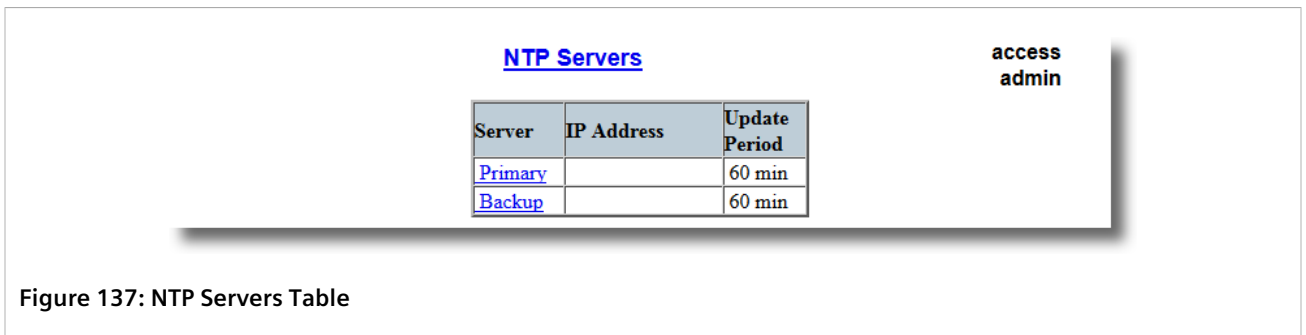
2. Select **Enabled** to enable SNTP, or select **Disabled** to disable SNTP.
3. Click **Apply**.

Section 9.2.2

## Configuring NTP Servers

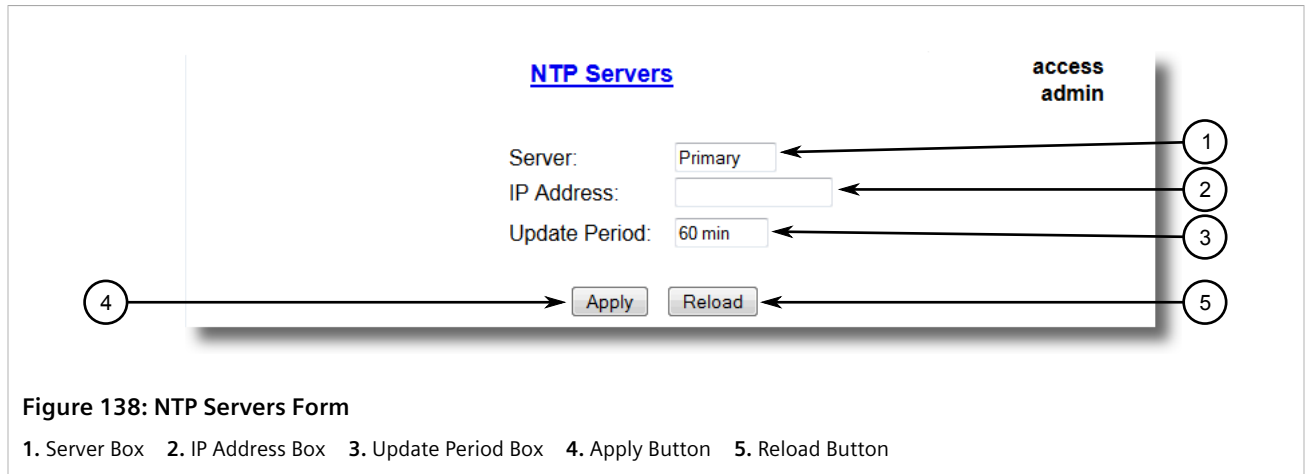
To configure either the primary or backup NTP server, do the following:

1. Navigate to **Administration » System Time Manager » Configure NTP » Configure NTP Servers**. The **NTP Servers** table appears.



**Figure 137: NTP Servers Table**

2. Select either **Primary** or **Backup**. The **NTP Servers** form appears.



**Figure 138: NTP Servers Form**

1. Server Box 2. IP Address Box 3. Update Period Box 4. Apply Button 5. Reload Button

3. Configure the following parameter(s) as required:

Parameter	Description
Server	<b>Synopsis:</b> Any 8 characters <b>Default:</b> Primary This field tells whether this configuration is for a Primary or a Backup Server.
IP Address	<b>Synopsis:</b> ###.###.###.### where ### ranges from 0 to 255 The Server IP Address.
Update Period	<b>Synopsis:</b> 1 to 1440 min <b>Default:</b> 60 min Determines how frequently the (S)NTP server is polled for a time update.If the server cannot be reached in three attempts that are made at one minute intervals an alarm is generated.

4. Click **Apply**.

# 10 Network Discovery and Management

RUGGEDCOM ROS supports the following protocols for automatic network discovery, monitoring and device management:

- **RUGGEDCOM Discovery Protocol (RCDP)**  
Use RCDP to discover RUGGEDCOM ROS-based devices over a Layer 2 network.
- **Link Layer Device Protocol (LLDP)**  
Use LLDP to broadcast the device's network capabilities and configuration to other devices on the network, as well as receive broadcasts from other devices.
- **Simple Network Management Protocol (SNMP)**  
Use SNMP to notify select users or groups of certain events that happen during the operation of the device, such as changes to network topology, link state, spanning tree root, etc.

## CONTENTS

- [Section 10.1, "Managing LLDP"](#)
- [Section 10.2, "Managing SNMP"](#)
- [Section 10.3, "ModBus Management Support"](#)

### Section 10.1

## Managing LLDP

The Link Layer Discovery Protocol (LLDP) defined by IEEE 802.11AB allows a networked device to advertise its own basic networking capabilities and configuration.

LLDP allows a networked device to discover its neighbors across connected network links using a standard mechanism. Devices that support LLDP are able to advertise information about themselves, including their capabilities, configuration, interconnections, and identifying information.

LLDP agent operation is typically implemented as two modules: the LLDP transmit module and LLDP receive module. The LLDP transmit module, when enabled, sends the local device's information at regular intervals, in IEEE 802.1AB standard format. Whenever the transmit module is disabled, it transmits an LLDPDU (LLDP data unit) with a time-to-live (TTL) type-length-value (TLV) containing 0 in the information field. This enables remote devices to remove the information associated with the local device in their databases. The LLDP receive module, when enabled, receives remote devices' information and updates its LLDP database of remote systems. When new or updated information is received, the receive module initiates a timer for the valid duration indicated by the TTL TLV in the received LLDPDU. A remote system's information is removed from the database when an LLDPDU is received from it with TTL TLV containing 0 in its information field.

**NOTE**  
LLDP is implemented to keep a record of only one device per Ethernet port. Therefore, if there are multiple devices sending LLDP information to a switch port on which LLDP is enabled, information about the neighbor on that port will change constantly.

**CONTENTS**

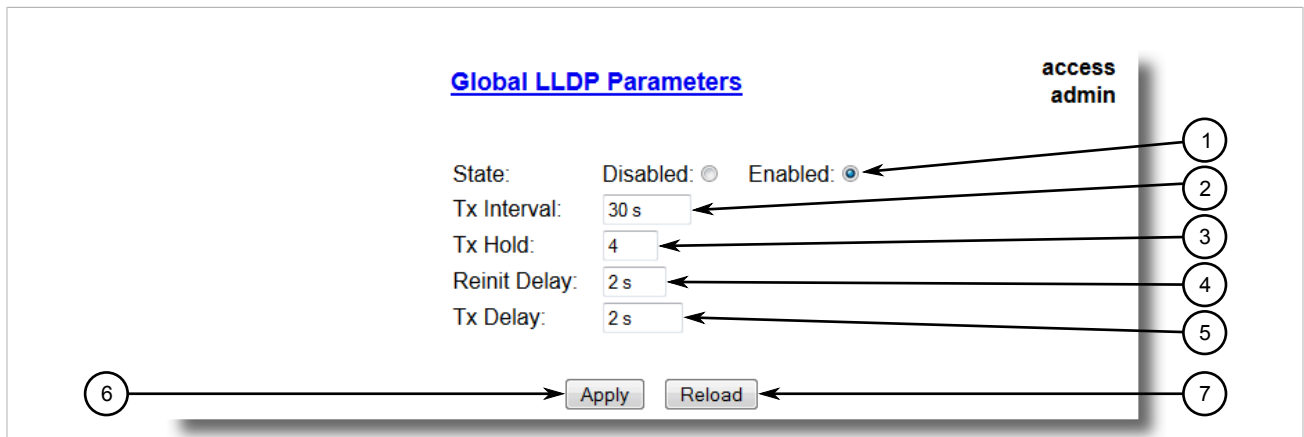
- Section 10.1.1, "Configuring LLDP Globally"
- Section 10.1.2, "Configuring LLDP for an Ethernet Port"
- Section 10.1.3, "Viewing Global Statistics and Advertised System Information"
- Section 10.1.4, "Viewing Statistics for LLDP Neighbors"
- Section 10.1.5, "Viewing Statistics for LLDP Ports"

Section 10.1.1

# Configuring LLDP Globally

To configure the global settings for LLDP, do the following:

1. Navigate to **Network Discovery » Link Layer Discovery Protocol » Configure Global LLDP Parameters**. The **Global LLDP Parameters** form appears.



**Figure 139: Global LLDP Parameters Form**

1. State Options 2. Tx Interval Box 3. Tx Hold Box 4. Reinit Delay Box 5. Tx Delay Box 6. Apply Button 7. Reload Button

2. Configure the following parameter(s) as required:

Parameter	Description
State	<b>Synopsis:</b> { Disabled, Enabled } <b>Default:</b> Enabled Enables LLDP protocol. Note that LLDP is enabled on a port when LLDP is enabled globally and along with enabling per port setting in Port LLDP Parameters menu.
Tx Interval	<b>Synopsis:</b> 5 to 32768 s <b>Default:</b> 30 s The interval at which LLDP frames are transmitted on behalf of this LLDP agent.

Parameter	Description
Tx Hold	<p><b>Synopsis:</b> 2 to 10 <b>Default:</b> 4</p> <p>The multiplier of the Tx Interval parameter that determines the actual time-to-live (TTL) value used in a LLDPDU. The actual TTL value can be expressed by the following formula:</p> <pre>TTL = MIN(65535, (Tx Interval * Tx Hold))</pre>
Reinit Delay	<p><b>Synopsis:</b> 1 to 10 s <b>Default:</b> 2 s</p> <p>The delay in seconds from when the value of Admin Status parameter of a particular port becomes 'Disabled' until re-initialization will be attempted.</p>
Tx Delay	<p><b>Synopsis:</b> 1 to 8192 s <b>Default:</b> 2 s</p> <p>The delay in seconds between successive LLDP frame transmissions initiated by value or status changed. The recommended value is set by the following formula:</p> <pre>1 &lt;= txDelay &lt;= (0.25 * Tx Interval)</pre>

3. Click **Apply**.

Section 10.1.2

## Configuring LLDP for an Ethernet Port

To configure LLDP for a specific Ethernet Port, do the following:

1. Navigate to **Network Discovery » Link Layer Discovery Protocol » Configure Port LLDP Parameters**. The **Port LLDP Parameters** table appears.

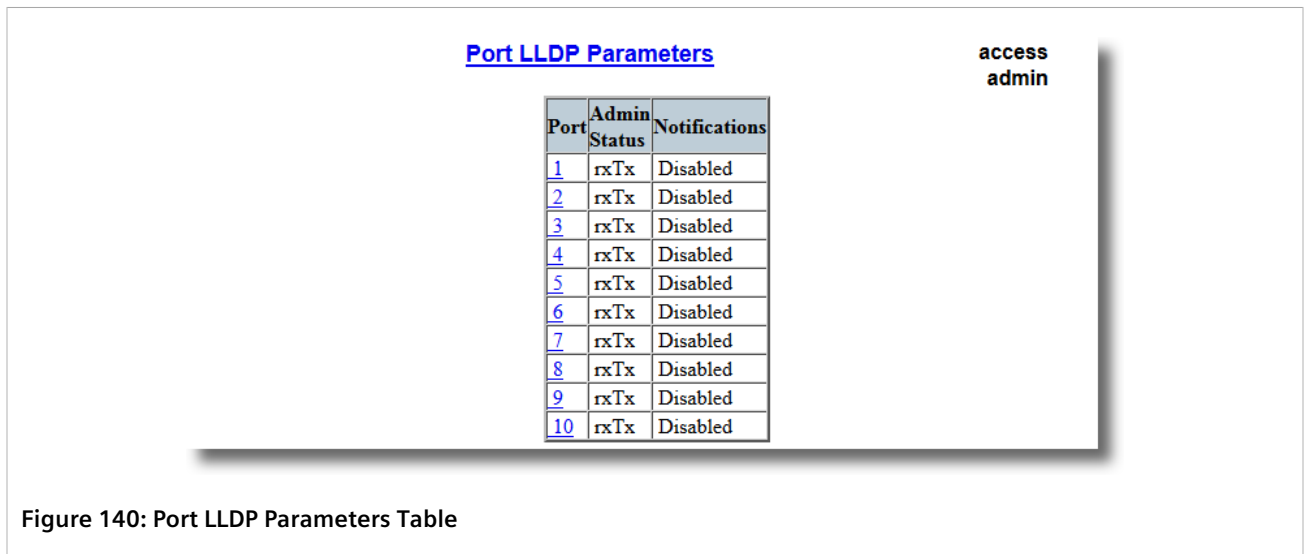
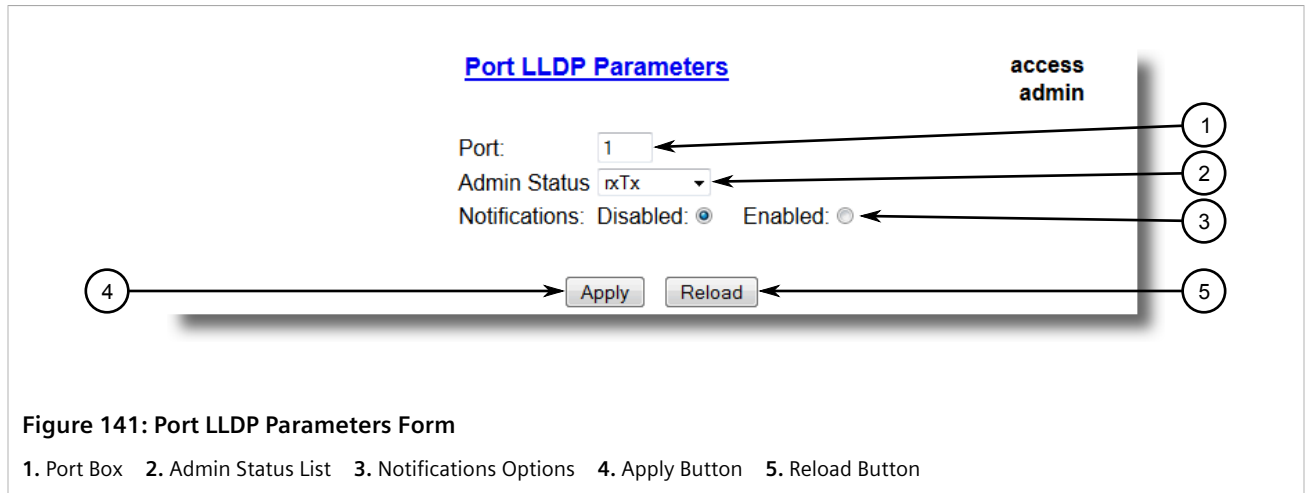


Figure 140: Port LLDP Parameters Table

2. Select a port. The **Port LLDP Parameters** form appears.



**Figure 141: Port LLDP Parameters Form**

1. Port Box   2. Admin Status List   3. Notifications Options   4. Apply Button   5. Reload Button

3. Configure the following parameter(s) as required:

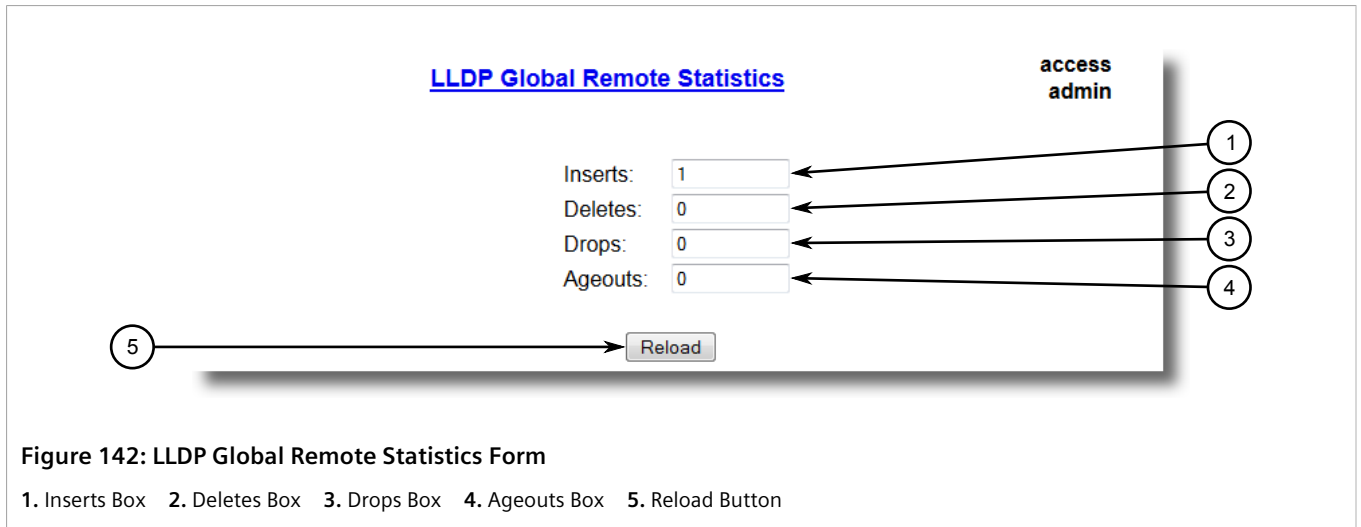
Parameter	Description
Port	<p><b>Synopsis:</b> 1 to maximum port number  <b>Default:</b> 1</p> <p>The port number as seen on the front plate silkscreen of the switch.</p>
Admin Status	<p><b>Synopsis:</b> { rxTx, txOnly, rxOnly, Disabled }  <b>Default:</b> rxTx</p> <p>rxTx: the local LLDP agent can both transmit and receive LLDP frames through the port.  txOnly: the local LLDP agent can only transmit LLDP frames.  rxOnly: the local LLDP agent can only receive LLDP frames.  disabled: the local LLDP agent can neither transmit or receive LLDP frames.</p>
Notifications	<p><b>Synopsis:</b> { Disabled, Enabled }  <b>Default:</b> Disabled</p> <p>Disabling notifications will prevent sending notifications and generating alarms for particular port from the LLDP agent.</p>

4. Click **Apply**.

Section 10.1.3

## Viewing Global Statistics and Advertised System Information

To view global statistics for LLDP and the system information that is advertised to neighbors, navigate to **Network Discovery » Link Layer Discovery Protocol » View LLDP Global Remote Statistics**. The **LLDP Global Remote Statistics** form appears.



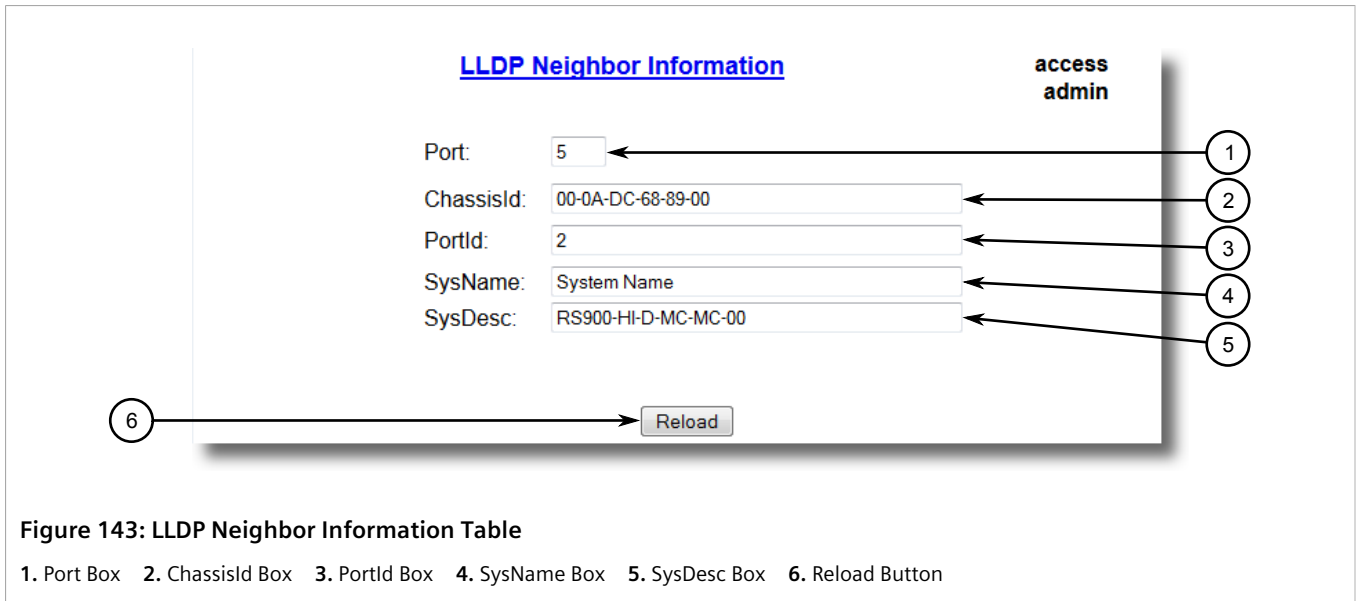
This form displays the following information:

Parameter	Description
Inserts	<b>Synopsis:</b> 0 to 4294967295 A number of times the entry in LLDP Neighbor Information Table was inserted.
Deletes	<b>Synopsis:</b> 0 to 4294967295 A number of times the entry in LLDP Neighbor Information Table was deleted.
Drops	<b>Synopsis:</b> 0 to 4294967295 A number of times an entry was deleted from LLDP Neighbor Information Table because the information timeliness interval has expired.
Ageouts	<b>Synopsis:</b> 0 to 4294967295 A counter of all TLVs discarded.

Section 10.1.4

## Viewing Statistics for LLDP Neighbors

To view statistics for LLDP neighbors, navigate to *Network Discovery » Link Layer Discovery Protocol » View LLDP Neighbor Information*. The LLDP Neighbor Information table appears.



This form displays the following information:

Parameter	Description
Port	<b>Synopsis:</b> 1 to maximum port number The local port associated with this entry.
ChassisId	<b>Synopsis:</b> Any 45 characters Chassis Id information received from remote LLDP agent.
PortId	<b>Synopsis:</b> Any 45 characters Port Id information received from remote LLDP agent.
SysName	<b>Synopsis:</b> Any 45 characters System Name information received from remote LLDP agent.
SysDesc	<b>Synopsis:</b> Any 45 characters System Descriptor information received from remote LLDP agent.

Section 10.1.5

## Viewing Statistics for LLDP Ports

To view statistics for LLDP ports, navigate to **Network Discovery » Link Layer Discovery Protocol » View LLDP Statistics**. The **LLDP Statistics** table appears.



<u>LLDP Statistics</u>							access admin
Port	FrmDrop	ErrFrm	FrmIn	FrmOut	Ageouts	TLVsDrop	TLVsUnknown
<a href="#">1</a>	0	0	12274	2041	1	0	36822
<a href="#">2</a>	0	0	2046	2041	1	0	0
<a href="#">3</a>	0	0	0	0	0	0	0
<a href="#">4</a>	0	0	0	0	0	0	0
<a href="#">5</a>	0	0	0	0	0	0	0
<a href="#">6</a>	0	0	0	0	0	0	0
<a href="#">7</a>	0	0	0	0	0	0	0
<a href="#">8</a>	0	0	1435	1433	0	0	0
<a href="#">9</a>	0	0	0	0	0	0	0
<a href="#">10</a>	0	0	0	0	0	0	0

Figure 144: LLDP Statistics Table

This table displays the following information:

Parameter	Description
Port	<b>Synopsis:</b> 1 to maximum port number The port number as seen on the front plate silkscreen of the switch.
FrmDrop	<b>Synopsis:</b> 0 to 4294967295 A counter of all LLDP frames discarded.
ErrFrm	<b>Synopsis:</b> 0 to 4294967295 A counter of all LLDPDUs received with detectable errors.
FrmIn	<b>Synopsis:</b> 0 to 4294967295 A counter of all LLDPDUs received.
FrmOut	<b>Synopsis:</b> 0 to 4294967295 A counter of all LLDPDUs transmitted.
Ageouts	<b>Synopsis:</b> 0 to 4294967295 A counter of the times that a neighbor's information has been deleted from the LLDP remote system MIB because the txinfoTTL timer has expired.
TLVsDrop	<b>Synopsis:</b> 0 to 4294967295 A counter of all TLVs discarded.
TLVsUnknown	<b>Synopsis:</b> 0 to 4294967295 A counter of all TLVs received on the port that are not recognized by the LLDP local agent.

Section 10.2

## Managing SNMP



**IMPORTANT!**

*SNMPv1, SNMPv2 and SNMPv3 are disabled by default in RUGGEDCOM ROS. To meet varied customer needs, these protocols can be enabled, but enabling them will break compliance with FIPS 140-2.*

*For more information, refer to the **FIPS 140-2 Non-Proprietary Security Policy** or contact Siemens Customer Support.*

RUGGEDCOM ROS supports versions 1, 2 and 3 of the Simple Network Management Protocol (SNMP), otherwise referred to as SNMPv1, SNMPv2c and SNMPv3 respectively. SNMPv3 provides secure access to the devices through a combination of authentication and packet encryption over the network. Security features for this protocol include:

Feature	Description
Message Integrity	Makes sure that a packet has not been tampered with in-transit.
Authentication	Determines if the message is from a valid source.
Encryption	Encrypts the contents of a packet to prevent it from being seen by an unauthorized source.

SNMPv3 provides security models and security levels. A security model is an authentication strategy setup for a user and the group in which the user resides. A security level is a permitted level of security within a security model. A combination of a security model and level will determine which security mechanism is employed when handling an SNMP packet.

Before configuring SNMPv3, note the following:

- Each user belongs to a group
- A group defines the access policy for a set of users
- An access policy defines what SNMP objects can be accessed for (i.e. reading, writing and creating notifications)
- A group determines the list of notifications its users can receive
- A group also defines the security model and security level for its users

For SNMPv1 and SNMPv2c, a community string can be configured. The string is mapped to the group and access level with a security name, which is configured as **User Name**.

#### CONTENTS

- [Section 10.2.1, "SNMP Management Interface Base \(MIB\) Support"](#)
- [Section 10.2.2, "SNMP Traps"](#)
- [Section 10.2.3, "Managing SNMP Users"](#)
- [Section 10.2.4, "Managing Security-to-Group Mapping"](#)
- [Section 10.2.5, "Managing SNMP Groups"](#)

#### Section 10.2.1

## SNMP Management Interface Base (MIB) Support

RUGGEDCOM ROS supports a variety of standard MIBs, proprietary RUGGEDCOM MIBs and Agent Capabilities MIBs, all for SNMP (Simple Network Management Protocol).

#### CONTENTS

- [Section 10.2.1.1, "Supported Standard MIBs"](#)
- [Section 10.2.1.2, "Supported Proprietary RUGGEDCOM MIBs"](#)
- [Section 10.2.1.3, "Supported Agent Capabilities"](#)

## Section 10.2.1.1

## Supported Standard MIBs

RUGGEDCOM ROS supports the following standard MIBs:

Standard	MIB Name	Title
RFC 2578	SNMPv2-SMI	Structure of Management Information Version 2
RFC 2579	SNMPv2-TC	Textual conventions for SMIv2
RFC 2580	SNMPv2-CONF	Conformance statements for SMIv2
	IANAifType	Enumerated values of the ifType Object Defined ifTable defined in IF-MIB
RFC 1907	SNMPv2-MIB	Management Information Base for SNMPv2
RFC 2011	IP-MIB	SNMPv2 Management Information Base for Internet Protocol using SMIv2
RFC 2012	TCP-MIB	SNMPv2 Management Information Base for the Transmission Control Protocol using SMIv2
RFC 2013	UDP-MIB	Management Information Base for the UDP using SMIv2
RFC 1659	RS-232-MIB	Definitions of managed objects for RS-232-like hardware devices
RFC 2863	IF-MIB	The Interface Group MIB
RFC 2819	RMON-MIB	Remote Network Monitoring (RMON) management Information base
RFC 4188	BRIDGE-MIB	Definitions of managed objects for bridges
RFC 4318	RSTP-MIB	Definitions of managed objects for bridges with Rapid Spanning Tree Protocol (RSTP)
RFC 3411	SNMP-FRAMEWORK-MIB	An architecture for describing Simple Network Management Protocol (SNMP) Management Framework
RFC 3414	SNMP-USER-BASED-SM-MIB	User-based Security Model (USM) for Version 3 of the Simple Network Management Protocol (SNMPv3)
RFC 3415	SNMP-VIEW-BASED-ACM-MIB	View-based Access Control Model (VACM) for the Simple Management Protocol (SNMP)
IEEE 802.3ad	IEEE8023-LAG-MIB	Management Information Base Module for link aggregation
IEEE 802.1AB-2005	LLDP-MIB	Management Information Base Module for LLDP configuration, statistics, local system data and remote systems data components
RFC 4363	Q-BRIDGE-MIB	Definitions of Managed Objects for Bridges with traffic classes, multicast filtering, and virtual LAN extensions

## Section 10.2.1.2

## Supported Proprietary RUGGEDCOM MIBs

RUGGEDCOM ROS supports the following proprietary RUGGEDCOM MIBs:

File Name	MIB Name	Description
RUGGEDCOM-MIB.mib	RUGGEDCOM-MIB	RUGGEDCOM enterprise SMI
RUGGEDCOM-TRAPS-MIB.mib	RUGGEDCOM-TRAPS-MIB	RUGGEDCOM traps definition

File Name	MIB Name	Description
RUGGEDCOM-SYS-INFO-MIB.mib	RUGGEDCOM-SYS-INFO-MIB	General system information about RUGGEDCOM device
RUGGEDCOM-DOT11-MIB.mib	RUGGEDCOM-DOT11-MIB	Management for wireless interface on RUGGEDCOM device
RUGGEDCOM-POE-MIB.mib	RUGGEDCOM-POE-MIB	Management for PoE ports on RUGGEDCOM device
RUGGEDCOM-SERIAL-MIB.mib	RUGGEDCOM-SERIAL-MIB	Management for serial ports on RUGGEDCOM device
RUGGEDCOM-STP-MIB.mib	RUGGEDCOM-STP-MIB	Management for RSTP protocol
RUGGEDCOM-NTP-MIB.mib	RUGGEDCOM-NTP-MIB	RUGGEDCOM proprietary MIB to control and monitor NTP module

Section 10.2.1.3

## Supported Agent Capabilities

RUGGEDCOM ROS supports the following agent capabilities for the SNMP agent:



**NOTE**

*For information about agent capabilities for SNMPv2, refer to [RFC 2580](http://tools.ietf.org/html/rfc2580) [<http://tools.ietf.org/html/rfc2580>].*

File Name	MIB Name	Supported MIB
RC-SNMPv2-MIB-AC.mib	RC-SNMPv2-MIB-AC	SNMPv2-MIB
RC-UDP-MIB-AC.mib	RC-UDP-MIB-AC	UDP-MIB
RC-TCP-MIB-AC.mib	RC-TCP-MIB-AC	TCP-MIB
RC-SNMP-USER-BASED-SM-MIB-AC.mib	RC-SNMP-USER-BASED-SM-MIB-AC	SNMP-USER-BASED-SM-MIB-AC
RC-SNMP-VIEW-BASED-ACM-MIB-AC.mib	RC-SNMP-VIEW-BASED-ACM-MIB-AC	SNMP-VIEW-BASED-ACM-MIB-AC
RC-IF-MIB-AC.mib	RC-IF-MIB-AC	IF-MIB
RC-BRIDGE-MIB-AC.mib	RC-BRIDGE-MIB-AC	BRIDGE-MIB
RC-RMON-MIB-AC.mib	RC-RMON-MIB-AC	RMON-MIB
RC-Q-BRIDGE-MIB-AC.mib	RC-Q-BRIDGE-MIB-AC	Q-BRIDGE-MIB
RC-IP-MIB-AC.mib	RC-IP-MIB-AC	IP-MIB
RC-LLDP-MIB-AC.mib	RC-LLDP-MIB-AC	LLDP-MIB
RC-LAG-MIB-AC.mib	RC-LAG-MIB-AC	IEEE8023-LAG-MIB
RC_RSTP-MIB-AC.mib	RC_RSTP-MIB-AC	RSTP-MIB
RC-RUGGEDCOM-DOT11-MIB-AC.mib	RC-RUGGEDCOM-DOT11-MIB-AC	RUGGEDCOM-DOT11- MIB
RC-RUGGEDCOM-POE-MIB-AC.mib	RC-RUGGEDCOM-POE-MIB-AC	RUGGEDCOM-POE-MIB
RC-RUGGEDCOM-STP-AC-MIB.mib	RC-RUGGEDCOM-STP-AC-MIB	RUGGEDCOM-STP-MIB
RC-RUGGEDCOM-SYS-INFO-MIB-AC.mib	RC-RUGGEDCOM-SYS-INFO-MIB-AC	RUGGEDCOM-SYS-INFO-MIB

File Name	MIB Name	Supported MIB
RC-RUGGEDCOM-TRAPS-MIB-AC.mib	RC-RUGGEDCOM-TRAPS-MIB-AC	RUGGEDCOM-TRAPS-MIB
RUGGEDCOM_RS-232-MIB-AC.mib	RUGGEDCOM_RS-232-MIB-AC	RS-232-MIB
RC-RUGGEDCOM-SERIAL-MIB-AC.mib	RC-RUGGEDCOM-SERIAL-MIB-AC	RUGGEDCOM-SERIAL-MIB
RC-NTP-MIB-AC.mib	RC-NTP-MIB-AC	NTP-MIB

Section 10.2.2

## SNMP Traps

The device generates the following traps.

### » Standard Traps

Trap	MIB
linkDown	IF-MIB
linkUp	
authenticationFailure	SNMPv2-MIB
coldStart	
newRoot	BRIDGE-MIB
topologyChage	
risingAlarm	RMON-MIB
fallingAlarm	
IldpRemoteTablesChange	LLDP-MIB

### » Specific Proprietary Traps

Trap	MIB
genericTrap	RUGGEDCOM-TRAPS-MIB
powerSupplyTrap	
swUpgradeTrap	
cfgChangeTrap	
weakPasswordTrap	
defaultKeysTrap	
privKeySnmpV3UserUnknwnTrap	
serialCommBlockedTrap	
unknownRouteSerialProto	
incopatableFpgaTrap	

Trap	MIB
clockMngrTrap	
ieee1588Trap	
rcLoopedBpduRcvd	
rcBpduGuardActivated	
rcGMRPCannotLearMoreAddresses	
rcGVRPCannotLearMoreAddresses	
rcMcastCpuFiltTblFull	
rclgmpGroupMembershipTblFull	
rclgmpMcastForwardTblFull	
rcMacAddressNotLearned	
excessLoginFailureTrap	
loginInfoTrap	
loginFailureTrap	
radiusServiceAvailableChange	
tacacsServiceAvailableChange	
rcDeviceError	
rcPortSecurityViolatedTrap	
rcMacAddrAuthFailedTrap	
rcRstpNewTopology	

### » Generic Proprietary Traps

Generic traps carry information about events in their severity and description objects. They are sent at the same time an alarm is generated for the device. The following are examples of RUGGEDCOM generic traps:



**NOTE**

Information about generic traps can be retrieved using the CLI command **alarms**. For more information about the **alarms** command, refer to [Section 2.5.1, "Available CLI Commands"](#).

Trap	Severity
TACACS+ response invalid	Warning
Unable to obtain IP address	Critical
SPP is rejected on Port 1	Error
BootP client: TFTP transfer failure	Error
received two consecutive confusing BPDUs on port, forcing down	Error

### » Event-Based Trap Examples

The device generates the following traps when specific events occur:

Trap	MIB	Event
rcPoeOverheat	RUGGEDCOM-POE-MIB	This trap is generated by a Power over Ethernet (PoE) overheat condition.
rcPoeOverload		This trap is generated by a Power over Ethernet (PoE) overload condition.

Section 10.2.3

## Managing SNMP Users

This section describes how to manage SNMP users.

### CONTENTS

- [Section 10.2.3.1, “Viewing a List of SNMP Users”](#)
- [Section 10.2.3.2, “Adding an SNMP User”](#)
- [Section 10.2.3.3, “Deleting an SNMP User”](#)

Section 10.2.3.1

### Viewing a List of SNMP Users

To view a list of SNMP users configured on the device, navigate to **Administration » Configure SNMP » Configure SNMP Users**. The **SNMP Users** table appears.

**access admin**

[InsertRecord](#)

Name	IP Address	v1/v2c Community	Auth Protocol	Priv Protocol	Auth
<a href="#">Manager</a>	192.168.0.100	Manager	HMACMD5	CBC-DES	xxxx
<a href="#">common</a>		common	noAuth	noPriv	
<a href="#">public</a>		public	noAuth	noPriv	
<a href="#">read</a>		public	noAuth	noPriv	

**Figure 145: SNMP Users Table**

If users have not been configured, add users as needed. For more information, refer to [Section 10.2.3.2, “Adding an SNMP User”](#).

Section 10.2.3.2

### Adding an SNMP User

Multiple users (up to a maximum of 32) can be configured for the local SNMPv3 engine, as well as SNMPv1 and SNMPv2c communities.

**NOTE**  
When employing the SNMPv1 or SNMPv2c security level, the **User Name** parameter maps the community name with the security group and access level.

To add a new SNMP user, do the following:

1. Navigate to **Administration » Configure SNMP » Configure SNMP Users**. The **SNMP Users** table appears.

The screenshot shows the 'SNMP Users' table with the following data:

Name	IP Address	v1/v2c Community	Auth Protocol	Priv Protocol	Auth
<a href="#">Manager</a>	192.168.0.100	Manager	HMACMD5	CBC-DES	xxx
<a href="#">common</a>		common	noAuth	noPriv	
<a href="#">public</a>		public	noAuth	noPriv	
<a href="#">read</a>		public	noAuth	noPriv	

Figure 146: SNMP Users Table

1. InsertRecord

2. Click **InsertRecord**. The **SNMP Users** form appears.

The screenshot shows the 'SNMP Users' form with the following fields and buttons:

- Name: initial
- IP Address: [ ]
- v1/v2c Community: [ ]
- Auth Protocol: noAuth
- Priv Protocol: noPriv (selected), CBC-DES
- Auth Key: [ ]
- Confirm Auth Key: [ ]
- Priv Key: [ ]
- Confirm Priv Key: [ ]
- Buttons: Apply, Delete, Reload

Figure 147: SNMP Users Form

1. Name Box
2. IP Address Box
3. v1/v2c Community Box
4. Auth Protocol Box
5. Priv Protocol Box
6. Auth Key Box
7. Confirm Auth Key Box
8. Priv Key Box
9. Confirm Priv Key Box
10. Apply Button
11. Delete Button
12. Reload Button





**NOTE**

RUGGEDCOM ROS requires that all user passwords meet strict guidelines to prevent the use of weak passwords. When creating a new password, make sure it adheres to the following rules:

- Must not be less than 6 characters in length.
- Must not include the username or any 4 continuous alphanumeric characters found in the username. For example, if the username is **Subnet25**, the password may not be **subnet25admin** or **subnetadmin**. However, **net25admin** or **Sub25admin** is permitted.
- Must have at least one alphabetic character and one number. Special characters are permitted.
- Must not have more than 3 continuously incrementing or decrementing numbers. For example, **Sub123** and **Sub19826** are permitted, but **Sub12345** is not.

An alarm will generate if a weak password is configured. The weak password alarm can be disabled by the user. For more information about disabling alarms, refer to [Section 5.4, "Managing Alarms"](#).

3. Configure the following parameter(s) as required:

Parameter	Description
Name	<b>Synopsis:</b> Any 32 characters <b>Default:</b> initial The name of the user. This user name also represents the security name that maps this user to the security group.
IP Address	<b>Synopsis:</b> ###.###.###.### where ### ranges from 0 to 255 The IP address of the user's SNMP management station. If IP address is configured, SNMP requests from that user will be verified by IP address as well. SNMP Authentication trap will be generated to trap receivers if request was received from this user, but from any other IP address. If IP address is empty, traps can not be generated to this user, but SNMP requests will be served for this user from any IP address.
v1/v2c Community	<b>Synopsis:</b> Any 32 characters The community string which is mapped by this user/security name to the security group if security model is SNMPv1 or SNMPv2c. If this string is left empty, it will be assumed to be equal to the same as user name.
Auth Protocol	<b>Synopsis:</b> { noAuth, HMACMD5, HMACSHA } <b>Default:</b> noAuth An indication of whether messages sent on behalf of this user to/from SNMP engine, can be authenticated, and if so, the type of authentication protocol which is used.
Priv Protocol	<b>Synopsis:</b> { noPriv, CBC-DES } <b>Default:</b> noPriv An Indication of whether messages sent on behalf of this user to/from SNMP engine can be protected from disclosure, and if so, the type of privacy protocol which is used.
Auth Key	<b>Synopsis:</b> 31 character ASCII string The secret authentication key (password) that must be shared with SNMP client. If the key is not an empty string, it must be at least 6 characters long.
Confirm Auth Key	<b>Synopsis:</b> 31 character ASCII string The secret authentication key (password) that must be shared with SNMP client. If the key is not an empty string, it must be at least 6 characters long.
Priv Key	<b>Synopsis:</b> 31 character ASCII string The secret encryption key (password) that must be shared with SNMP client. If the key is not an empty string, it must be at least 6 characters long.

Parameter	Description
Confirm Priv Key	<b>Synopsis:</b> 31 character ASCII string The secret encryption key (password) that must be shared with SNMP client. If the key is not an empty string, it must be at least 6 characters long.

- Click **Apply**.

Section 10.2.3.3

## Deleting an SNMP User

To delete an SNMP user, do the following:

- Navigate to **Administration » Configure SNMP » Configure SNMP Users**. The **SNMP Users** table appears.

**SNMP Users** access  
admin

[InsertRecord](#)

Name	IP Address	v1/v2c Community	Auth Protocol	Priv Protocol	Autl
<a href="#">Manager</a>	192.168.0.100	Manager	HMACMD5	CBC-DES	xxx
<a href="#">common</a>		common	noAuth	noPriv	
<a href="#">public</a>		public	noAuth	noPriv	
<a href="#">read</a>		public	noAuth	noPriv	

**Figure 148: SNMP Users Table**

- Select the user from the table. The **SNMP Users** form appears.

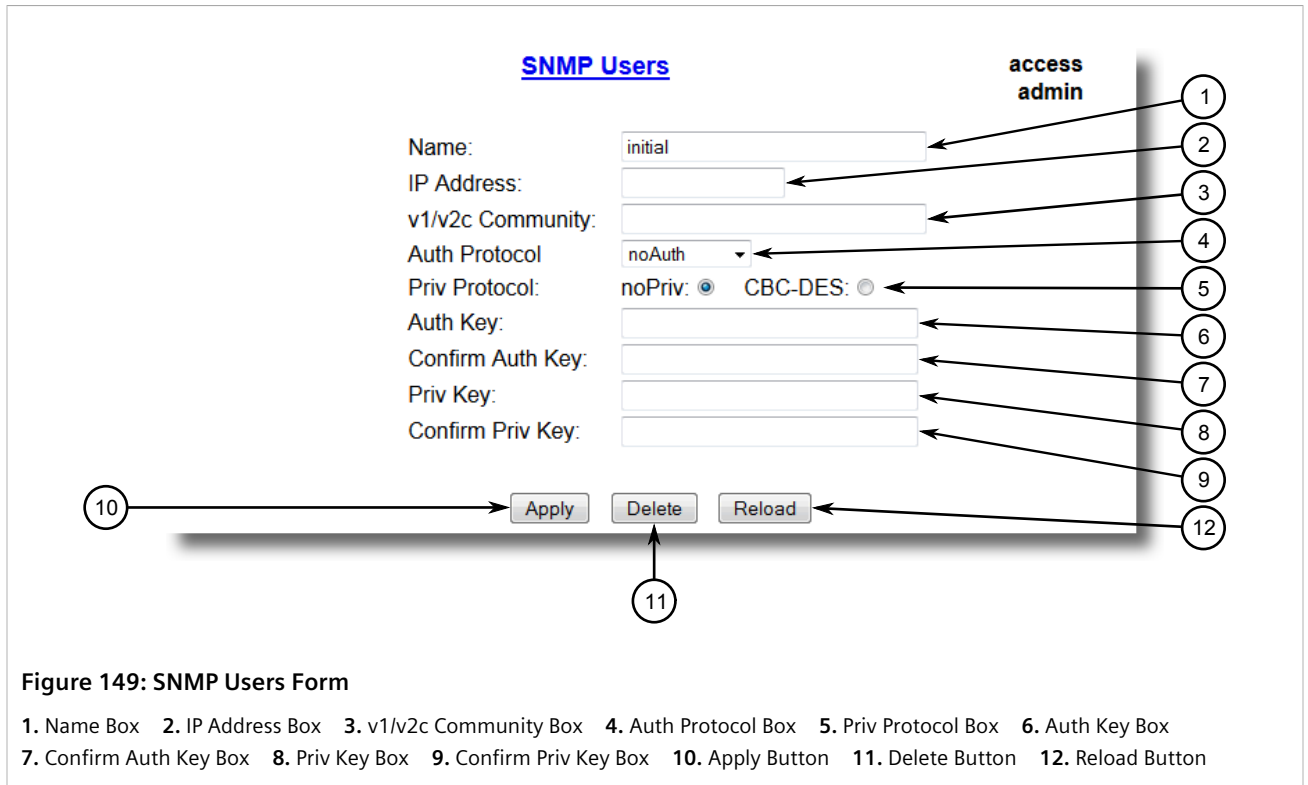


Figure 149: SNMP Users Form

1. Name Box 2. IP Address Box 3. v1/v2c Community Box 4. Auth Protocol Box 5. Priv Protocol Box 6. Auth Key Box  
7. Confirm Auth Key Box 8. Priv Key Box 9. Confirm Priv Key Box 10. Apply Button 11. Delete Button 12. Reload Button

3. Click **Delete**.

#### Section 10.2.4

## Managing Security-to-Group Mapping

This section describes how to configure and manage security-to-group maps.

### CONTENTS

- [Section 10.2.4.1, "Viewing a List of Security-to-Group Maps"](#)
- [Section 10.2.4.2, "Adding a Security-to-Group Map"](#)
- [Section 10.2.4.3, "Deleting a Security-to-Group Map"](#)

#### Section 10.2.4.1

### Viewing a List of Security-to-Group Maps

To view a list of security-to-group maps configured on the device, navigate to **Administration » Configure SNMP » Configure SNMP Security to Group Maps**. The **SNMP Security to Group Maps** table appears.

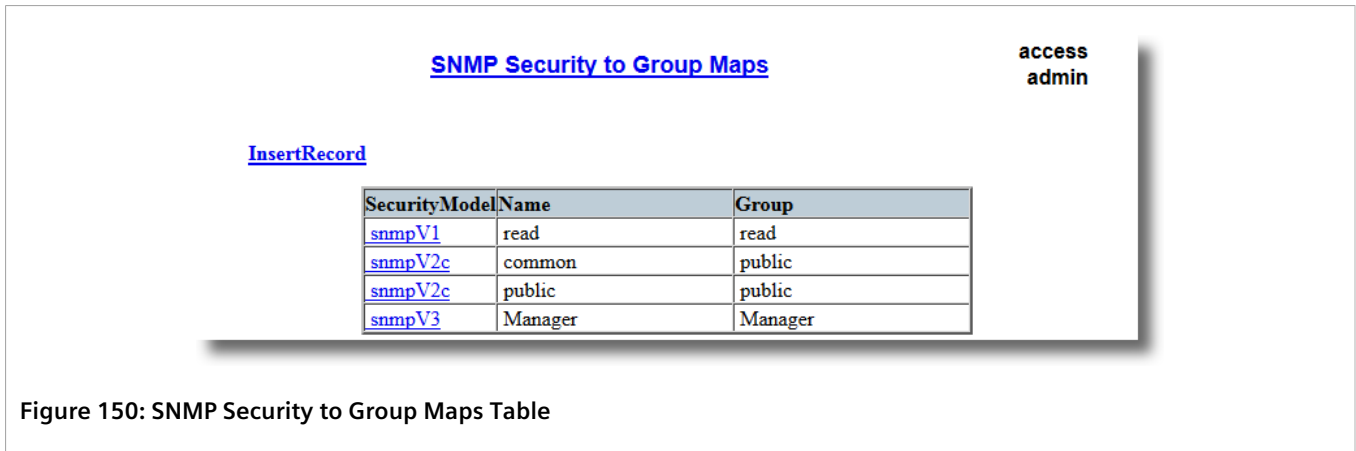


Figure 150: SNMP Security to Group Maps Table

If security-to-group maps have not been configured, add maps as needed. For more information, refer to Section 10.2.4.2, “Adding a Security-to-Group Map”.

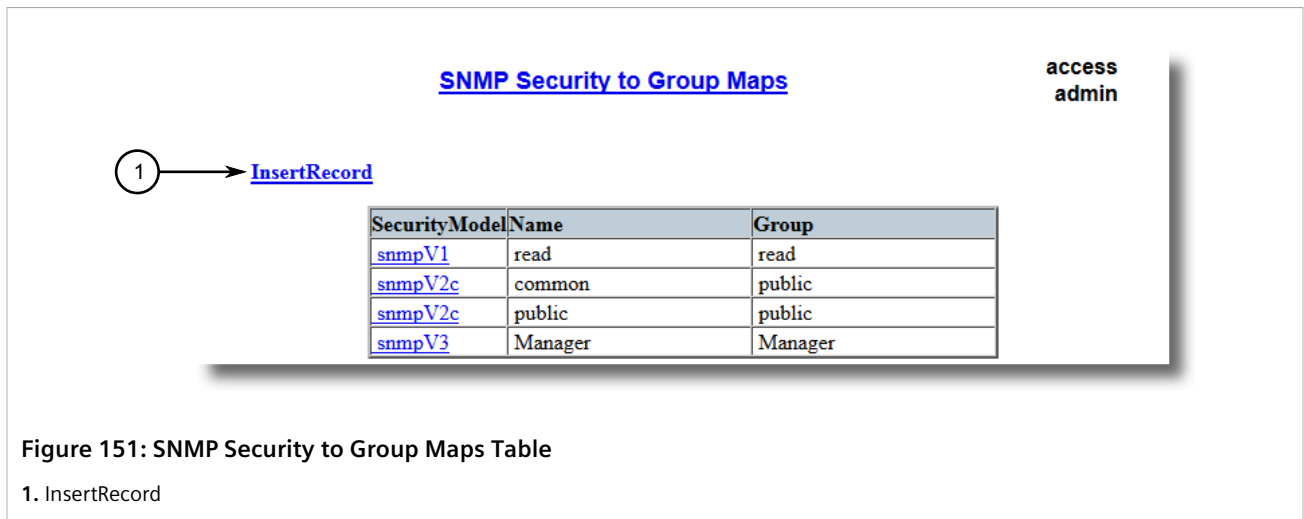
Section 10.2.4.2

## Adding a Security-to-Group Map

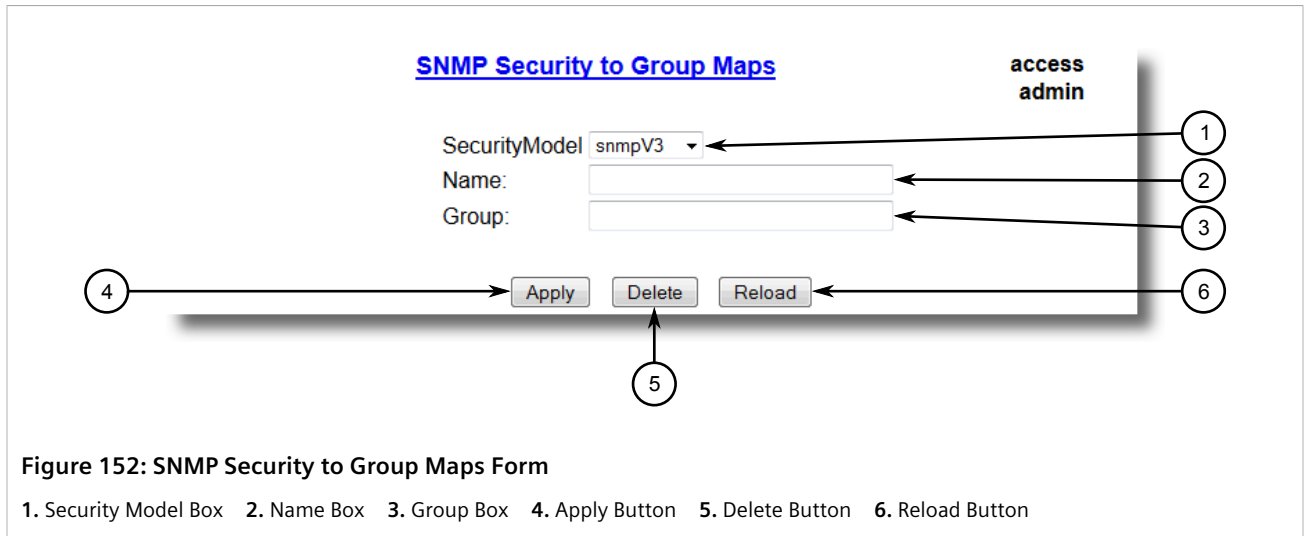
Multiple combinations of security models and groups can be mapped (up to a maximum of 32) for SNMP.

To add a security-to-group map, do the following:

1. Navigate to **Administration » Configure SNMP » Configure SNMP Security to Group Maps**. The **SNMP Security to Group Maps** table appears.



2. Click **InsertRecord**. The **SNMP Security to Group Maps** form appears.



- Configure the following parameter(s) as required:

Parameter	Description
SecurityModel	<b>Synopsis:</b> { snmpV1, snmpV2c, snmpV3 } <b>Default:</b> snmpV3 The Security Model that provides the name referenced in this table.
Name	<b>Synopsis:</b> Any 32 characters The user name which is mapped by this entry to the specified group name.
Group	<b>Synopsis:</b> Any 32 characters The group name to which the security model and name belong. This name is used as an index to the SNMPv3 VACM Access Table.

- Click **Apply**.

### Section 10.2.4.3

## Deleting a Security-to-Group Map

To delete a security-to-group map, do the following:

- Navigate to **Administration » Configure SNMP » Configure SNMP Security to Group Maps**. The **SNMP Security to Group Maps** table appears.

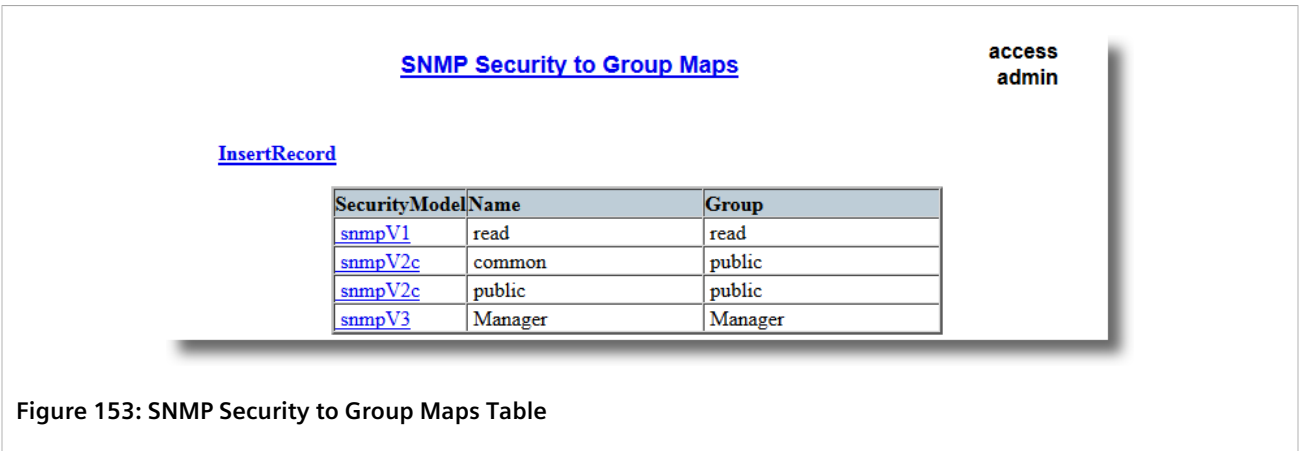


Figure 153: SNMP Security to Group Maps Table

2. Select the map from the table. The **SNMP Security to Group Maps** form appears.

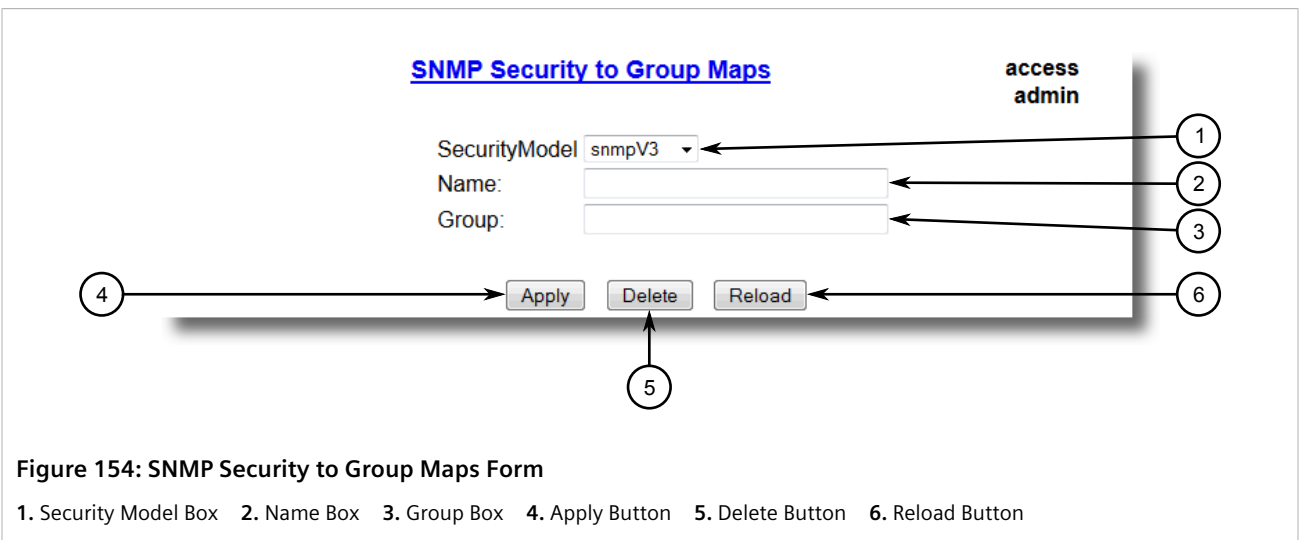


Figure 154: SNMP Security to Group Maps Form

1. Security Model Box
2. Name Box
3. Group Box
4. Apply Button
5. Delete Button
6. Reload Button

3. Click **Delete**.

Section 10.2.5

## Managing SNMP Groups

Multiple SNMP groups (up to a maximum of 32) can be configured to have access to SNMP.

### CONTENTS

- [Section 10.2.5.1, "Viewing a List of SNMP Groups"](#)
- [Section 10.2.5.2, "Adding an SNMP Group"](#)
- [Section 10.2.5.3, "Deleting an SNMP Group"](#)

Section 10.2.5.1

## Viewing a List of SNMP Groups

To view a list of SNMP groups configured on the device, navigate to **Administration » Configure SNMP » Configure SNMP Access**. The **SNMP Access** table appears.

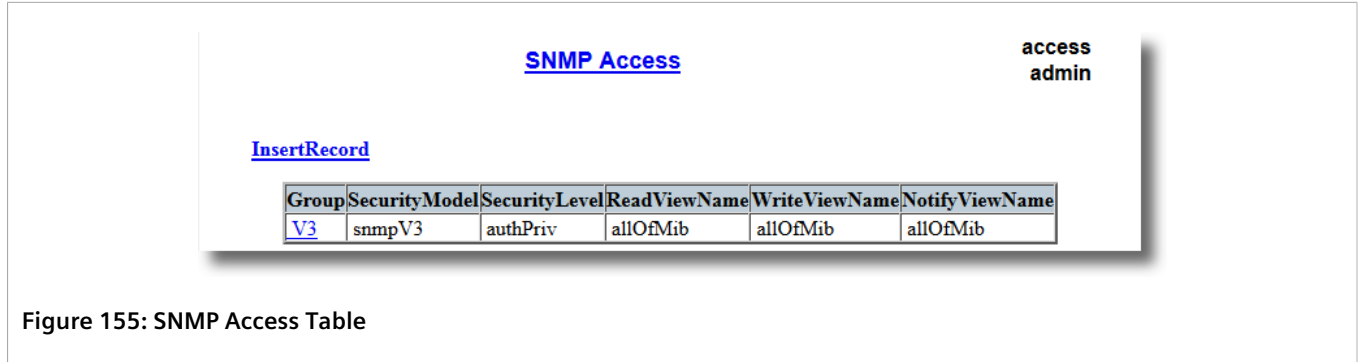


Figure 155: SNMP Access Table

If SNMP groups have not been configured, add groups as needed. For more information, refer to [Section 10.2.5.2, "Adding an SNMP Group"](#).

Section 10.2.5.2

## Adding an SNMP Group

To add an SNMP group, do the following:

1. Navigate to **Administration » Configure SNMP » Configure SNMP Access**. The **SNMP Access** table appears.

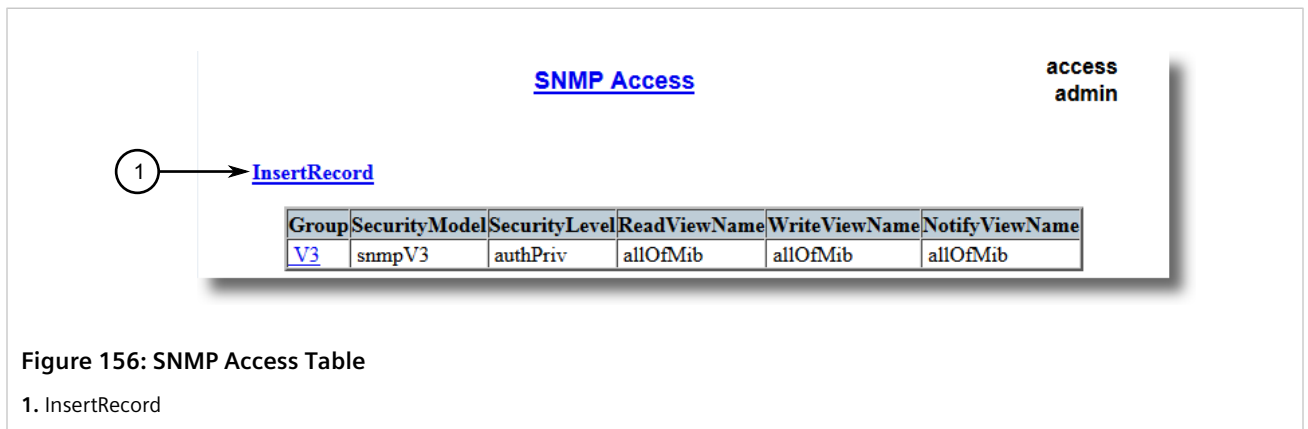
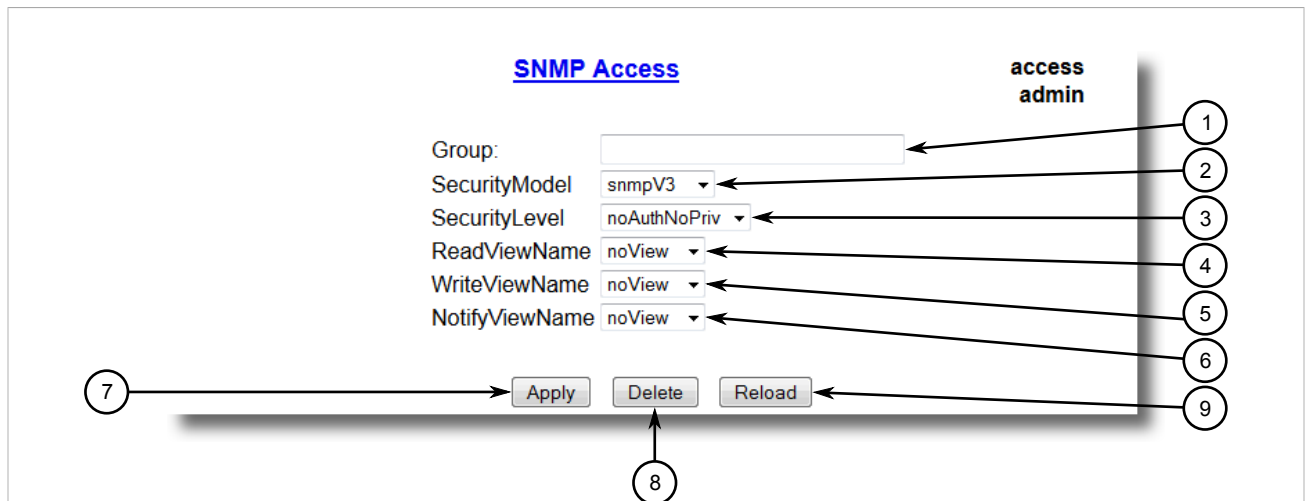


Figure 156: SNMP Access Table

1. InsertRecord

2. Click **InsertRecord**. The **SNMP Access** form appears.



**Figure 157: SNMP Access Form**

1. Group Box 2. Security Model Box 3. Security Level Box 4. ReadViewName Box 5. WriteViewName Box 6. NotifyViewName Box 7. Apply Button 8. Delete Button 9. Reload Button

3. Configure the following parameter(s) as required:

Parameter	Description
Group	<b>Synopsis:</b> Any 32 characters The group name to which the security model and name belong. This name is used as an index to the SNMPv3 VACM Access Table.
SecurityModel	<b>Synopsis:</b> { snmpV1, snmpV2c, snmpV3 } <b>Default:</b> snmpV3 To gain the access rights allowed by this entry, configured security model must be in use.
SecurityLevel	<b>Synopsis:</b> { noAuthNoPriv, authNoPriv, authPriv } <b>Default:</b> noAuthNoPriv The minimum level of security required to gain the access rights allowed by this entry. A security level of noAuthNoPriv is less than authNoPriv, which is less than authPriv.
ReadViewName	<b>Synopsis:</b> { noView, V1Mib, allOfMib } <b>Default:</b> noView This parameter identifies the MIB tree(s) to which this entry authorizes read access. If the value is noView, then no read access is granted.
WriteViewName	<b>Synopsis:</b> { noView, V1Mib, allOfMib } <b>Default:</b> noView This parameter identifies the MIB tree(s) to which this entry authorizes write access. If the value is noView, then no write access is granted.
NotifyViewName	<b>Synopsis:</b> { noView, V1Mib, allOfMib } <b>Default:</b> noView This parameter identifies the MIB tree(s) to which this entry authorizes access for notifications. If the value is noView, then no access for notifications is granted.

4. Click **Apply**.

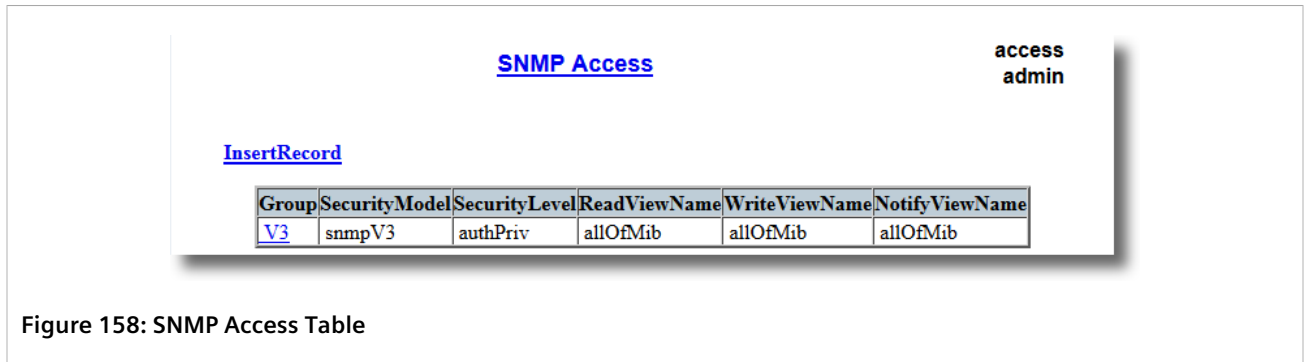


Section 10.2.5.3

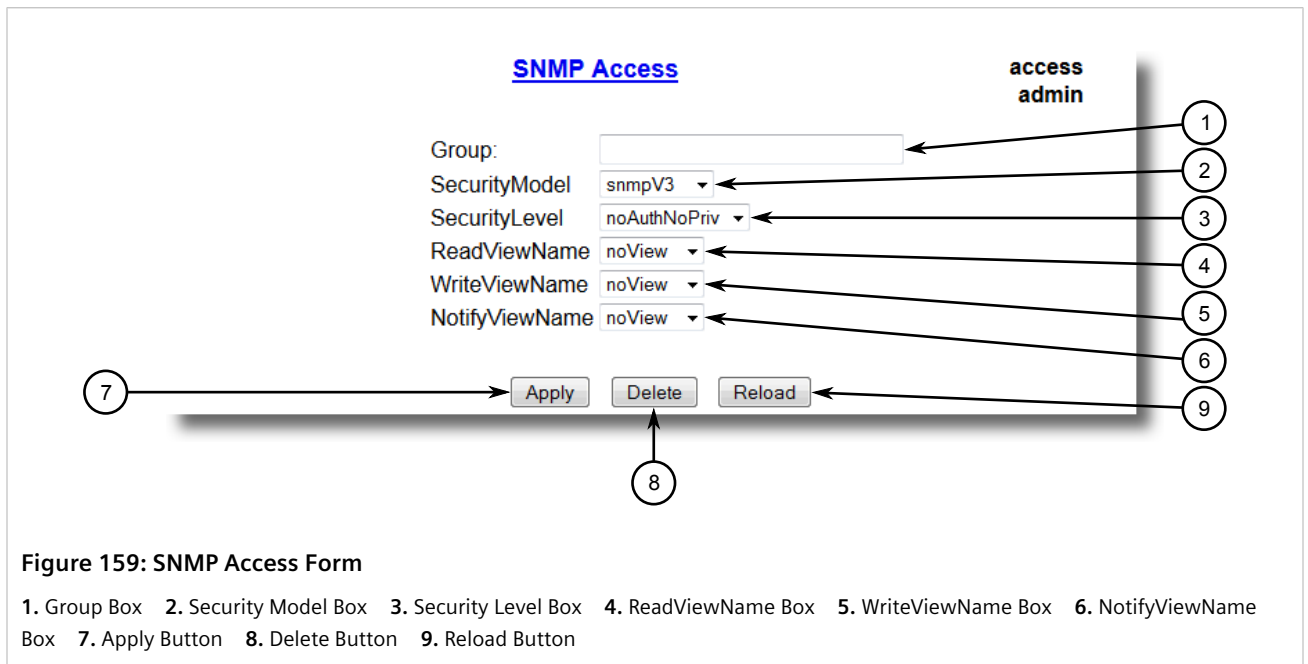
## Deleting an SNMP Group

To delete an SNMP group, do the following:

1. Navigate to **Administration » Configure SNMP » Configure SNMP Access**. The **SNMP Access** table appears.



2. Select the group from the table. The **SNMP Access** form appears.



3. Click **Delete**.

Section 10.3

## ModBus Management Support

Modbus management support in RUGGEDCOM devices provides a simple interface for retrieving basic status information. ModBus support simplifies the job of SCADA (Supervisory Control and Data Acquisition) system integrators by providing familiar protocols for retrieving RUGGEDCOM device information. ModBus provides mostly read-only status information, but there are some writeable registers for operator commands.

The ModBus protocol PDU (Protocol Data Unit) format is as follows:



**IMPORTANT!**

Modbus management interface is insecure and is disabled by default in RUGGEDCOM ROS. When enabled, compliance with FIPS will be broken. If Modbus management interface is required, then it is recommended to follow the security recommendations outlined in this User Guide and to configure the environment according to defense-in-depth best practices.

Function Code

Data

**CONTENTS**

- [Section 10.3.1, “ModBus Function Codes”](#)
- [Section 10.3.2, “ModBus Memory Map”](#)
- [Section 10.3.3, “Modbus Memory Formats”](#)

Section 10.3.1

## ModBus Function Codes

RUGGEDCOM devices support the following ModBus function codes for device management through ModBus:



**NOTE**

While RUGGEDCOM devices have a variable number of ports, not all registers and bits apply to all products.

Registers that are not applicable to a particular device return a zero (0) value. For example, registers referring to serial ports are not applicable to RUGGEDCOM switch devices.

### » Read Input Registers or Read Holding Registers — 0x04 or 0x03

Example PDU Request

Function Code	1 Byte	0x04(0x03)
Starting Address	2 Bytes	0x0000 to 0xFFFF (Hexadecimal) 128 to 65535 (Decimal)
Number of Input Registers	2 Bytes	Bytes 0x0001 to 0x007D

Example PDU Response

Function Code	1 Byte	0x04(0x03)
Byte Count	1 Byte	2 x N <sup>a</sup>
Number of Input Registers	N <sup>a</sup> x 2 Bytes	

<sup>a</sup> The number of input registers

### » Write Multiple Registers — 0x10

Example PDU Request

Function Code	1 Byte	0x10
---------------	--------	------

Starting Address	2 Bytes	0x0000 to 0xFFFF
Number of Input Registers	2 Bytes	Bytes 0x0001 to 0x0079
Byte Count	1 Byte	$2 \times N^b$
Registers Value	$N^b \times 2$ Bytes	Value of the register

<sup>b</sup>The number of input registers

#### Example PDU Response

Function Code	1 Byte	0x10
Starting Address	2 Bytes	0x0000 to 0xFFFF
Number of Registers	2 Bytes	1 to 121 (0x79)

### Section 10.3.2

## ModBus Memory Map

The following details how ModBus process variable data is mapped.

### » Product Info

The following data is mapped to the *Productinfo* table:

Address	#Registers	Description (Reference Table in UI)	R/W	Format
0000	16	Product Identification	R	Text
0010	32	Firmware Identification	R	Text
0040	1	Number of Ethernet Ports	R	Uint16
0041	1	Number of Serial Ports	R	Uint16
0042	1	Number of Alarms	R	Uint16
0043	1	Power Supply Status	R	PSStatusCmd
0044	1	FailSafe Relay Status	R	TruthValue
0045	1	ErrorAlarm Status	R	TruthValue

### » Product Write Register

The following data is mapped to various tables:

Address	#Registers	Description (Reference Table in UI)	R/W	Format
0080	1	Clear Alarms	W	Cmd
0081	2	Reset Ethernet Ports	W	PortCmd
0083	2	Clear Ethernet Statistics	W	PortCmd
0085	2	Reset Serial Ports	W	PortCmd
0087	2	Clear Serial Port Statistics	W	PortCmd

## » Alarms

The following data is mapped to the *alarms* table:

Address	#Registers	Description (Reference Table in UI)	R/W	Format
0100	64	Alarm 1	R	Alarm
0140	64	Alarm 2	R	Alarm
0180	64	Alarm 3	R	Alarm
01C0	64	Alarm 4	R	Alarm
0200	64	Alarm 5	R	Alarm
0240	64	Alarm 6	R	Alarm
0280	64	Alarm 7	R	Alarm
02C0	64	Alarm 8	R	Alarm

## » Ethernet Port Status

The following data is mapped to the *ethPortStats* table:

Address	#Registers	Description (Reference Table in UI)	R/W	Format
03FE	2	Port Link Status	R	PortCmd

## » Ethernet Statistics

The following data is mapped to the *rmonStats* table:

Address	#Registers	Description (Reference Table in UI)	R/W	Format
0400	2	Port 1 Statistics - Ethernet In Packets	R	UInt32
0402	2	Port 2 Statistics - Ethernet In Packets	R	UInt32
0404	2	Port 3 Statistics - Ethernet In Packets	R	UInt32
0406	2	Port 4 Statistics - Ethernet In Packets	R	UInt32
0408	2	Port 5 Statistics - Ethernet In Packets	R	UInt32
040A	2	Port 6 Statistics - Ethernet In Packets	R	UInt32
040C	2	Port 7 Statistics - Ethernet In Packets	R	UInt32
040E	2	Port 8 Statistics - Ethernet In Packets	R	UInt32
0410	2	Port 9 Statistics - Ethernet In Packets	R	UInt32
0412	2	Port 10 Statistics - Ethernet In Packets	R	UInt32
0414	2	Port 11 Statistics - Ethernet In Packets	R	UInt32
0416	2	Port 12 Statistics - Ethernet In Packets	R	UInt32
0418	2	Port 13 Statistics - Ethernet In Packets	R	UInt32
041A	2	Port 14 Statistics - Ethernet In Packets	R	UInt32
041C	2	Port 15 Statistics - Ethernet In Packets	R	UInt32

Address	#Registers	Description (Reference Table in UI)	R/W	Format
041E	2	Port 16 Statistics - Ethernet In Packets	R	Uint32
0420	2	Port 17 Statistics - Ethernet In Packets	R	Uint32
0422	2	Port 18 Statistics - Ethernet In Packets	R	Uint32
0424	2	Port 19 Statistics - Ethernet In Packets	R	Uint32
0426	2	Port 20 Statistics - Ethernet In Packets	R	Uint32
0440	2	Port 1 Statistics - Ethernet Out Packets	R	Uint32
0442	2	Port 2 Statistics - Ethernet Out Packets	R	Uint32
0444	2	Port 3 Statistics - Ethernet Out Packets	R	Uint32
0446	2	Port 4 Statistics - Ethernet Out Packets	R	Uint32
0448	2	Port 5 Statistics - Ethernet Out Packets	R	Uint32
044A	2	Port 6 Statistics - Ethernet Out Packets	R	Uint32
044C	2	Port 7 Statistics - Ethernet Out Packets	R	Uint32
044E	2	Port 8 Statistics - Ethernet Out Packets	R	Uint32
0450	2	Port 9 Statistics - Ethernet Out Packets	R	Uint32
0452	2	Port 10 Statistics - Ethernet Out Packets	R	Uint32
0454	2	Port 11 Statistics - Ethernet Out Packets	R	Uint32
0456	2	Port 12 Statistics - Ethernet Out Packets	R	Uint32
0458	2	Port 13 Statistics - Ethernet Out Packets	R	Uint32
045A	2	Port 14 Statistics - Ethernet Out Packets	R	Uint32
045C	2	Port 15 Statistics - Ethernet Out Packets	R	Uint32
045E	2	Port 16 Statistics - Ethernet Out Packets	R	Uint32
0460	2	Port 17 Statistics - Ethernet Out Packets	R	Uint32
0462	2	Port 18 Statistics - Ethernet Out Packets	R	Uint32
0464	2	Port 19 Statistics - Ethernet Out Packets	R	Uint32
0466	2	Port 20 Statistics - Ethernet Out Packets	R	Uint32
0480	2	Port 1 Statistics - Ethernet In Octets	R	Uint32
0482	2	Port 2 Statistics - Ethernet In Octets	R	Uint32
0484	2	Port 3 Statistics - Ethernet In Octets	R	Uint32
0486	2	Port 4 Statistics - Ethernet In Octets	R	Uint32
0488	2	Port 5 Statistics - Ethernet In Octets	R	Uint32
048A	2	Port 6 Statistics - Ethernet In Octets	R	Uint32
048C	2	Port 7 Statistics - Ethernet In Octets	R	Uint32
048E	2	Port 8 Statistics - Ethernet In Octets	R	Uint32
0490	2	Port 9 Statistics - Ethernet In Octets	R	Uint32

Address	#Registers	Description (Reference Table in UI)	R/W	Format
0492	2	Port 10 Statistics - Ethernet In Octets	R	Uint32
0494	2	Port 11 Statistics - Ethernet In Octets	R	Uint32
0496	2	Port 12 Statistics - Ethernet In Octets	R	Uint32
0498	2	Port 13 Statistics - Ethernet In Octets	R	Uint32
049A	2	Port 14 Statistics - Ethernet In Octets	R	Uint32
049C	2	Port 15 Statistics - Ethernet In Octets	R	Uint32
049E	2	Port 16 Statistics - Ethernet In Octets	R	Uint32
04A0	2	Port 17 Statistics - Ethernet In Octets	R	Uint32
04A2	2	Port 18 Statistics - Ethernet In Octets	R	Uint32
04A4	2	Port 19 Statistics - Ethernet In Octets	R	Uint32
04A6	2	Port 20 Statistics - Ethernet In Octets	R	Uint32
04C0	2	Port 1 Statistics - Ethernet Out Octets	R	Uint32
04C2	2	Port 2 Statistics - Ethernet Out Octets	R	Uint32
04C4	2	Port 3 Statistics - Ethernet Out Octets	R	Uint32
04C6	2	Port 4 Statistics - Ethernet Out Octets	R	Uint32
04C8	2	Port 5 Statistics - Ethernet Out Octets	R	Uint32
04CA	2	Port 6 Statistics - Ethernet Out Octets	R	Uint32
04CC	2	Port 7 Statistics - Ethernet Out Octets	R	Uint32
04CE	2	Port 8 Statistics - Ethernet Out Octets	R	Uint32
04D0	2	Port 9 Statistics - Ethernet Out Octets	R	Uint32
04D2	2	Port 10 Statistics - Ethernet Out Octets	R	Uint32
04D4	2	Port 11 Statistics - Ethernet Out Octets	R	Uint32
04D6	2	Port 12 Statistics - Ethernet Out Octets	R	Uint32
04D8	2	Port 13 Statistics - Ethernet Out Octets	R	Uint32
04DA	2	Port 14 Statistics - Ethernet Out Octets	R	Uint32
04DC	2	Port 15 Statistics - Ethernet Out Octets	R	Uint32
04DE	2	Port 16 Statistics - Ethernet Out Octets	R	Uint32
04E0	2	Port 17 Statistics - Ethernet Out Octets	R	Uint32
04E2	2	Port 18 Statistics - Ethernet Out Octets	R	Uint32
04E4	2	Port 19 Statistics - Ethernet Out Octets	R	Uint32
04E6	2	Port 20 Statistics - Ethernet Out Octets	R	Uint32

## » Serial Statistics

The following data is mapped to the *uartPortStatus* table:

Address	#Registers	Description (Reference Table in UI)	R/W	Format
0600	2	Port 1 Statistics – Serial In characters	R	Uint32
0602	2	Port 2 Statistics – Serial In characters	R	Uint32
0604	2	Port 3 Statistics – Serial In characters	R	Uint32
0606	2	Port 4 Statistics – Serial In characters	R	Uint32
0640	2	Port 1 Statistics – Serial Out characters	R	Uint32
0642	2	Port 2 Statistics – Serial Out characters	R	Uint32
0644	2	Port 3 Statistics – Serial Out characters	R	Uint32
0646	2	Port 4 Statistics – Serial Out characters	R	Uint32
0680	2	Port 1 Statistics – Serial In Packets	R	Uint32
0682	2	Port 2 Statistics – Serial In Packets	R	Uint32
0684	2	Port 3 Statistics – Serial In Packets	R	Uint32
0686	2	Port 4 Statistics – Serial In Packets	R	Uint32
06C0	2	Port 1 Statistics – Serial Out Packets	R	Uint32
06C2	2	Port 2 Statistics – Serial Out Packets	R	Uint32
06C4	2	Port 3 Statistics – Serial Out Packets	R	Uint32
06C6	2	Port 4 Statistics – Serial Out Packets	R	Uint32

Section 10.3.3

## Modbus Memory Formats

This section defines the Modbus memory formats supported by RUGGEDCOM ROS.

### CONTENTS

- [Section 10.3.3.1, "Text"](#)
- [Section 10.3.3.2, "Cmd"](#)
- [Section 10.3.3.3, "Uint16"](#)
- [Section 10.3.3.4, "Uint32"](#)
- [Section 10.3.3.5, "PortCmd"](#)
- [Section 10.3.3.6, "Alarm"](#)
- [Section 10.3.3.7, "PSStatusCmd"](#)
- [Section 10.3.3.8, "TruthValues"](#)

Section 10.3.3.1

## Text

The Text format provides a simple ASCII representation of the information related to the product. The most significant register byte of an ASCII characters comes first.

For example, consider a *Read Multiple Registers* request to read Product Identification from location 0x0000.

0x04	0x00	0x00	0x00	0x08
------	------	------	------	------

The response may look like:

0x04	0x10	0x53	0x59	0x53	0x54	0x45	0x4D	0x20	0x4E	0x41	0x4D	0x45
0x00	0x00	0x00	0x00	0x00								

In this example, starting from byte 3 until the end, the response presents an ASCII representation of the characters for the product identification, which reads as *SYSTEM NAME*. Since the length of this field is smaller than eight registers, the rest of the field is filled with zeros (0).

Section 10.3.3.2

## Cmd

The Cmd format instructs the device to set the output to either *true* or *false*. The most significant byte comes first.

- FF 00 hex requests output to be True
- 00 00 hex requests output to be False
- Any value other than the suggested values does not affect the requested operation

For example, consider a *Write Multiple Registers* request to clear alarms in the device.

0x10	0x00	0x80	0x00	0x01	2	0xFF	0x00
------	------	------	------	------	---	------	------

- FF 00 for register 00 80 clears the system alarms
- 00 00 does not clear any alarms

The response may look like:

0x10	0x00	0x80	0x00	0x01
------	------	------	------	------

Section 10.3.3.3

## Uint16

The Uint16 format describes a Standard ModBus 16 bit register.

Section 10.3.3.4

## Uint32

The Uint32 format describes Standard 2 ModBus 16 bit registers. The first register holds the most significant 16 bits of a 32 bit value. The second register holds the least significant 16 bits of a 32 bit value.



## Section 10.3.3.5

## PortCmd

The PortCmd format describes a bit layout per port, where 1 indicates the requested action is true, and 0 indicates the requested action is false.

PortCmd provides a bit layout of a maximum of 32 ports. Therefore, it uses two ModBus registers:

- The first ModBus register corresponds to ports 1 – 16
- The second ModBus register corresponds to ports 17 – 32 for a particular action

Bits that do not apply to a particular product are always set to zero (0).

A bit value of 1 indicates that the requested action is true. For example, the port is *up*.

A bit value of 0 indicates that the requested action is false. For example, the port is *down*.

### » Reading Data Using PortCmd

To understand how to read data using PortCmd, consider a ModBus Request to read multiple registers from location 0x03FE.

0x04	0x03	0xFE	0x00	0x02
------	------	------	------	------

The response depends on how many ports are available on the device. For example, if the maximum number of ports on a connected RUGGEDCOM device is 20, the response would be similar to the following:

0x04	0x04	0xF2	0x76	0x00	0x05
------	------	------	------	------	------

In this example, bytes 3 and 4 refer to register 1 at location 0x03FE, and represent the status of ports 1 – 16. Bytes 5 and 6 refer to register 2 at location 0x03FF, and represent the status of ports 17 – 32. The device only has 20 ports, so byte 6 contains the status for ports 17 – 20 starting from right to left. The rest of the bits in register 2 corresponding to the non-existing ports 21 – 31 are zero (0).

### » Performing Write Actions Using PortCmd

To understand how data is written using PortCmd, consider a Write Multiple Register request to clear Ethernet port statistics:

0x10	0x00	0x83	0x00	0x01	2	0x55	0x76	0x00	0x50
------	------	------	------	------	---	------	------	------	------

A bit value of 1 clears Ethernet statistics on the corresponding port. A bit value of 0 does not clear the Ethernet statistics.

0x10	0x00	0x81	0x00	0x02
------	------	------	------	------

## Section 10.3.3.6

## Alarm

The Alarm format is another form of text description. Alarm text corresponds to the alarm description from the table holding all of the alarms. Similar to the Text format, this format returns an ASCII representation of alarms.



**NOTE**

*Alarms are stacked in the device in the sequence of their occurrence (i.e. Alarm 1, Alarm 2, Alarm 3, etc.).*

The first eight alarms from the stack can be returned, if they exist. A zero (0) value is returned if an alarm does not exist.

Section 10.3.3.7

**PSStatusCmd**

The PSStatusCmd format describes a bit layout for providing the status of available power supplies. Bits 0-4 of the lower byte of the register are used for this purpose.

- Bits 0-1: Power Supply 1 Status
- Bits 2-3: Power Supply 2 Status

Other bits in the register do not provide any system status information.

Bit Value	Description
01	Power Supply not present (01 = 1)
10	Power Supply is functional (10 = 2)
11	Power Supply is not functional (11 = 3)

The values used for power supply status are derived from the RUGGEDCOM-specific SNMP MIB.

» **Reading the Power Supply Status from a Device Using PSStatusCmd**

To understand how to read the power supply status from a device using PSStatusCmd, consider a ModBus Request to read multiple registers from location 0x0043.

0x04	0x00	0x43	0x00	0x01
------	------	------	------	------

The response may look like:

0x04	0x02	0x00	0x0A
------	------	------	------

The lower byte of the register displays the power supply's status. In this example, both power supplies in the unit are functional.

Section 10.3.3.8

**TruthValues**

The Truthvalues format represents a true or false status in the device:

- 1 indicates the corresponding status for the device to be true
- 2 indicates the corresponding status for the device to be false

### » Reading the FailSafe Relay Status From a Device Using TruthValue

To understand how to use the TruthValue format to read the FailSafe Relay status from a device, consider a ModBus request to read multiple registers from location 0x0044.

0x04	0x00	0x44	0x00	0x01
------	------	------	------	------

The response may look like:

0x04	0x02	0x00	0x01
------	------	------	------

The register's lower byte shows the FailSafe Relay status. In this example, the FailSafe Relay is energized.

### » Reading the ErrorAlarm Status From a Device Using TruthValue

To understand how to use the TruthValue format to read the ErrorAlarm status from a device, consider a ModBus request to read multiple registers from location 0x0045.

0x04	0x00	0x45	0x00	0x01
------	------	------	------	------

The response may look like:

0x04	0x02	0x00	0x01
------	------	------	------

The register's lower byte shows the ErrorAlarm status. In this example, there is no active ERROR, ALERT or CRITICAL alarm in the device.



# 11 IP Address Assignment

This chapter describes features related to the assignment of IP addresses.

## CONTENTS

- [Section 11.1, “Configuring the DHCP Relay Agent”](#)

### Section 11.1

## Configuring the DHCP Relay Agent

A DHCP Relay Agent is a device that forwards DHCP packets between clients and servers when they are not on the same physical LAN segment or IP subnet. The feature is enabled if the DHCP server IP address and a set of access ports are configured.

DHCP Option 82 provides a mechanism for assigning an IP Address based on the location of the client device in the network. Information about the client’s location can be sent along with the DHCP request to the server. Based on this information, the DHCP server makes a decision about an IP Address to be assigned.

DHCP Relay Agent takes the broadcast DHCP requests from clients received on the configured access port and inserts the relay agent information option (Option 82) into the packet. Option 82 contains the VLAN ID (2 bytes) and the port number of the access port (2 bytes: the circuit ID sub-option) and the switch’s MAC address (the remote ID sub-option). This information uniquely defines the access port’s position in the network. For example, the Circuit ID for VLAN 1 on port 1 is 00:01:00:01.

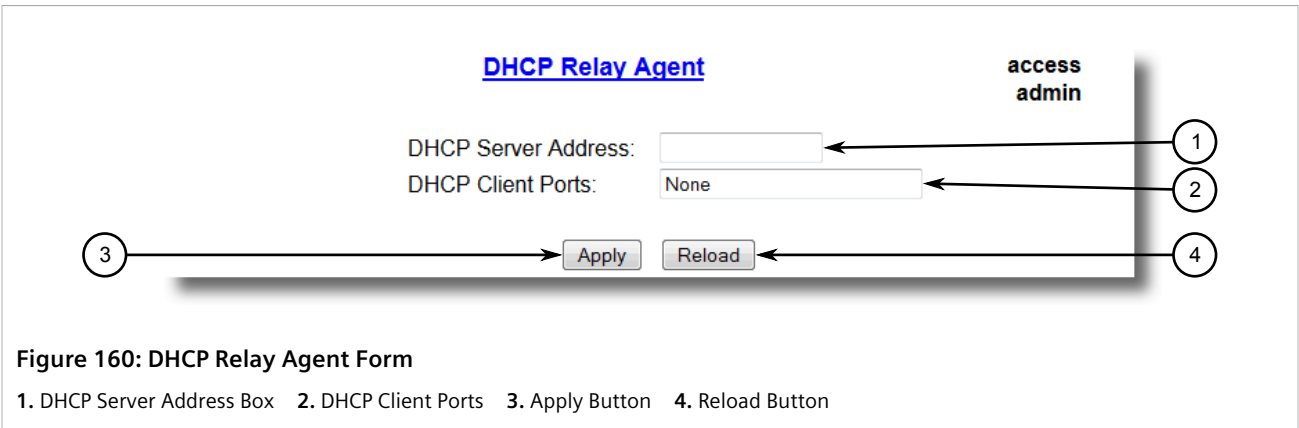
The DHCP Server supporting DHCP Option 82 sends a unicast reply and echoes Option 82. The DHCP Relay Agent removes the Option 82 field and broadcasts the packet to the port from which the original request was received.

These parameters provide the ability to configure the switch to act as a relay agent for DHCP Option 82.

The DHCP Relay Agent communicates to the server on a management interface. The agent’s IP address is the address configured for the management interface.

To configure the DHCP Relay Agent, do the following:

1. Navigate to **Administration » Configure DHCP Relay Agent**. The **DHCP Relay Agent** form appears.



2. Configure the following parameter(s) as required:

Parameter	Description
DHCP Server Address	<p><b>Synopsis:</b> ###.###.###.### where ### ranges from 0 to 255</p> <p><b>Default:</b></p> <p>This parameter specifies the IP address of the DHCP server to which DHCP queries will be forwarded from this relay agent.</p>
DHCP Client Ports	<p><b>Synopsis:</b> Any combination of numbers valid for this parameter</p> <p><b>Default:</b> None</p> <p>This parameter specifies ports where DHCP clients are connected.</p> <p>Examples:</p> <ul style="list-style-type: none"> <li>• All - all ports of the switch can have DHCP clients connected.</li> <li>• 2,4-6,8 - ports 2,4,5,6 and 8 can have DHCP clients connected</li> </ul>

3. Click **Apply**.

# 12 Troubleshooting

This chapter describes troubleshooting steps for common issues that may be encountered when using RUGGEDCOM ROS or designing a network.



**IMPORTANT!**

*For further assistance, contact a Customer Service representative.*

**CONTENTS**

- [Section 12.1, "General"](#)
- [Section 12.2, "Ethernet Ports"](#)
- [Section 12.3, "Spanning Tree"](#)
- [Section 12.4, "VLANs"](#)

Section 12.1

## General

The following describes common problems.

Problem	Solution
<p>The switch is not responding to ping attempts, even though the IP address and gateway have been configured. The switch is receiving the ping because the LEDs are flashing and the device statistics are logging the pings. What is going on?</p>	<p>Is the switch being pinged through a router? If so, the switch gateway address must be configured as well. The following figure illustrates the problem.</p> <div data-bbox="654 1314 1531 1619"> </div> <p><b>Figure 161: Using a Router As a Gateway</b>                      1. Work Station 2. Router 3. Switch</p>

The router is configured with the appropriate IP subnets and will forward the ping from the workstation to the switch. When the switch responds, however, it will not know which of its interfaces to use to reach the workstation and will drop the response. Programming a gateway of 10.0.0.1 will cause the switch to forward unresolvable frames to the router.

Problem	Solution
	This problem will also occur if the gateway address is not configured and the switch tries to raise an SNMP trap to a host that is not on the local subnet.

## Section 12.2

## Ethernet Ports

The following describes common problems related to Ethernet ports.

Problem	Solution
A link seems fine when traffic levels are low, but fails as traffic rates increase OR a link can be pinged but has problems with FTP/SQL/ HTTP/etc.	<p>A possible cause of intermittent operation is that of a 'duplex mismatch'. If one end of the link is fixed to full-duplex and the peer auto-negotiates, the auto-negotiating end falls back to half-duplex operation.</p> <p>At lower traffic volumes, the link may display few if any errors. As the traffic volume rises, the fixed negotiation side will begin to experience dropped packets while the auto-negotiating side will experience collisions. Ultimately, as traffic loads approach 100%, the link will become entirely unusable.</p> <p>The ping command with flood options is a useful tool for testing commissioned links. The command <code>ping 192.168.0.1 500 2</code> can be used to issue 500 pings each separated by two milliseconds to the next switch. If the link used is of high quality, then no pings should be lost and the average round trip time should be small.</p>
Links are inaccessible, even when using the Link Fault Indication (LFI) protection feature.	Make sure LFI is not enabled on the peer as well. If both sides of the link have LFI enabled, then both sides will withhold link signal generation from each other.

## Section 12.3

## Spanning Tree

The following describes common problems related to the Spanning Tree Protocol (STP).

Problem	Solution
The network locks up when a new port is connected and the port status LEDs are flashing rapidly.	Is it possible that one of the switches in the network or one of the ports on a switch in the network has STP disabled and accidentally connects to another switch? If this has occurred, then a traffic loop has been formed.
Occasionally, the ports seem to experience significant flooding for a brief period of time.	If the problem appears to be transient in nature, it is possible that ports that are part of the spanning tree have been configured as edge ports. After the link layers have come up on edge ports, STP will directly transition them (perhaps improperly) to the forwarding state. If an RSTP configuration message is then received, the port will be returned to blocking. A traffic loop may be formed for the length of time the port was in forwarding.
A switch displays a strange behavior where the root port hops back and forth between two switch ports and never settles down.	<p>If one of the switches appears to flip the root from one port to another, the problem may be one of traffic prioritization. For more information refer to <a href="#">"The network becomes unstable when a specific application is started."</a></p> <p>Another possible cause of intermittent operation is that of an auto-negotiation mismatch. If one end of the link is fixed to full-duplex mode and the peer auto-negotiates, the auto-negotiating end will fall back to half-duplex operation. At lower traffic, the volumes the link may display few if any errors. As the traffic volume rises, the fixed negotiation side will begin to experience dropped packets while the auto-negotiating side will experience collisions. Ultimately, as traffic loads approach 100%, the link will become entirely unusable. At this point, RSTP will not be able to transmit configuration messages over the link and the spanning tree topology will break down. If an alternate trunk exists, RSTP will activate it in the place of the congested port. Since activation of the alternate port often relieves the congested port of its traffic, the congested port will once again become reliable. RSTP will</p>




Problem	Solution
	promptly enter it back into service, beginning the cycle once again. The root port will flip back and forth between two ports on the switch.
A computer or device is connected to a switch. After the switch is reset, it takes a long time for it to come up.	<p>Is it possible that the RSTP edge setting for this port is set to false? If Edge is set to false, the bridge will make the port go through two forward delay times before the port can send or receive frames. If Edge is set to true, the bridge will transition the port directly to forwarding upon link up.</p> <p>Another possible explanation is that some links in the network run in half-duplex mode. RSTP uses a peer-to-peer protocol called Proposal-Agreement to ensure transitioning in the event of a link failure. This protocol requires full-duplex operation. When RSTP detects a non-full duplex port, it cannot rely on Proposal-Agreement protocol and must make the port transition the slow (i.e. STP) way. If possible, configure the port for full-duplex operation. Otherwise, configure the port's point-to-point setting to true.</p> <p>Either one will allow the Proposal-Agreement protocol to be used.</p>
When the switch is tested by deliberately breaking a link, it takes a long time before devices beyond the switch can be polled.	<p>Is it possible that some ports participating in the topology have been configured to STP mode or that the port's point-to-point parameter is set to false? STP and multipoint ports converge slowly after failures occur.</p> <p>Is it possible that the port has migrated to STP? If the port is connected to the LAN segment by shared media and STP bridges are connected to that media, then convergence after link failure will be slow.</p> <p>Delays on the order of tens or hundreds of milliseconds can result in circumstances where the link broken is the sole link to the root bridge and the secondary root bridge is poorly chosen. The worst of all possible designs occurs when the secondary root bridge is located at the farthest edge of the network from the root. In this case, a configuration message will have to propagate out to the edge and then back to reestablish the topology.</p>
The network is composed of a ring of bridges, of which two (connected to each other) are managed and the rest are unmanaged. Why does the RSTP protocol work quickly when a link is broken between the managed bridges, but not in the unmanaged bridge part of the ring?	A properly operating unmanaged bridge is transparent to STP configuration messages. The managed bridges will exchange configuration messages through the unmanaged bridge part of the ring as if it is non-existent. When a link in the unmanaged part of the ring fails however, the managed bridges will only be able to detect the failure through timing out of hello messages. Full connectivity will require three hello times plus two forwarding times to be restored.
The network becomes unstable when a specific application is started. The network returns to normal when the application is stopped.	RSTP sends its configuration messages using the highest possible priority level. If CoS is configured to allow traffic flows at the highest priority level and these traffic flows burst continuously to 100% of the line bandwidth, STP may be disrupted. It is therefore advised not to use the highest CoS.
When a new port is brought up, the root moves on to that port instead of the port it should move to or stay on.	Is it possible that the port cost is incorrectly programmed or that auto-negotiation derives an undesired value? Inspect the port and path costs with each port active as root.
An Intelligent Electronic Device (IED) or controller does not work with the device.	<p>Certain low CPU bandwidth controllers have been found to behave less than perfectly when they receive unexpected traffic. Try disabling STP for the port.</p> <p>If the controller fails around the time of a link outage, there is the remote possibility that frame disordering or duplication may be the cause of the problem. Try setting the root port of the failing controller's bridge to STP.</p>
Polls to other devices are occasionally lost.	Review the network statistics to determine whether the root bridge is receiving Topology Change Notifications (TCNs) around the time of observed frame loss. It may be possible there are problems with intermittent links in the network.
The root is receiving a number of TCNs. Where are they coming from?	Examine the RSTP port statistics to determine the port from which the TCNs are arriving. Sign-on to the switch at the other end of the link attached to that port. Repeat this step until the switch generating the TCNs is found (i.e. the switch that is itself not receiving a large number of TCNs). Determine the problem at that switch.

Section 12.4

# VLANs

The following describes common problems related to the VLANs.

Problem	Solution
VLANs are not needed on the network. Can they be turned off?	Yes. Simply leave all ports set to type <i>edge</i> and leave the native VLAN set to 1. This is the default configuration for the switch.
Two VLANs were created and a number of ports were made members of them. Now some of the devices in one VLAN need to send messages to devices in the other VLAN.	If the devices need to communicate at the physical address layer, they must be members of the same VLAN. If they can communicate in a Layer 3 fashion (i.e. using a protocol such as IP or IPX), use a router. The router will treat each VLAN as a separate interface, which will have its own associated IP address space.
On a network of 30 switches, management traffic needs to be restricted to a separate domain. What is the best method for doing this while staying in contact with these switches?	<p>At the switch where the management station is located, configure a port to use the new management VLAN as its native VLAN. Configure a host computer to act as a temporary management station.</p> <p>At each switch, configure the management VLAN to the new value. Contact with each individual switch will be lost immediately as they are being configured, but it should be possible re-establish communication from the temporary management station. After all switches have been taken to the new management VLAN, configure the ports of all attached management devices to use the new VLAN.</p> <div data-bbox="609 846 1481 963" style="border: 1px solid gray; padding: 5px;"> <p> <b>NOTE</b>  <i>Establishing a management domain is often accompanied with the establishment of an IP subnet specifically for the managed devices.</i></p> </div>